TRINITY NETWORX LLC
MASTER SERVICE AGREEMENT
MSA Version: 08-14-2026.002

This Master Client Services Agreement (this "Agreement") is between TRINITY NETWORX LLC, a limited liability corporation that maintains an office for business at 3281 E. Guasti Rd., Ste 700, Ontario, CA 91761 ("**Company**"), and ##CustomerOrganization##, that maintains an office for business at ##CustomerStreetAddress##, ##CustomerCity##, CA ##CustomerPostalCode## ("**Client**").

The Agreement shall be effective for a month-to-month period, beginning on the Commencement Date, which is determined by the date noted below under "Commencement Date." This agreement renews monthly and can be terminated by either party with ninety (90) days' written notice. The recipient of this document and signing pursuant to the accepted quote will be the primary contact person and email used for any and all information about this Agreement.

Commencement Date: ##QuoteCreatedDate##

Client: ##CustomerOrganization##

THE PARTIES AGREE TO THE FOLLOWING:

1. SCOPE OF SERVICES.

Trinity Networx, LLC, referred to in this Agreement as the "Company," shall provide the managed information technology and related professional services selected by Client and identified in the applicable service-plan exhibit incorporated into this Agreement. The available service plans are: Exhibit 1, Trinity Foundation; Exhibit 2, Trinity Complete; and Exhibit 3, Trinity Complete Secure. The service-plan exhibit selected and executed by Client is referred to as the "Service Plan."

The Service Plan defines the allocation of information technology responsibilities between Company and Client, the services included in Client's recurring fees, applicable service limitations, and services that require separate authorization or additional charges. Only the Service Plan expressly identified in the applicable Order, Quote, or signature page shall apply to Client.

Company may also provide projects, consulting, remediation, installation, migration, emergency response, and other services under one or more separately authorized statements of work, quotes, proposals, work orders, or change orders, each of which is referred to as a "Statement of Work." Each Statement of Work must reference this Agreement or otherwise demonstrate the parties' intent that it be governed by this Agreement. Upon authorization by both parties, the Statement of Work shall become part of and be governed by this Agreement.

Unless expressly stated otherwise, recurring fees under the Service Plan cover only the services specifically identified as included in the selected Service Plan. Hardware, software, subscriptions, licenses, third-party services, projects, onsite work, after-hours services, remediation, and other items not expressly included shall be separately quoted or billed at Company's then-current rates.

In the event of a direct conflict among the documents governing the Services, the following order of precedence shall apply: first, a Statement of Work, but only regarding the specific project or services addressed in that Statement of Work; second, the applicable Service Plan; third, the main body of this Agreement; and fourth, any other quote, proposal, or supporting document. A Statement of Work shall not modify the main body of this Agreement or the applicable Service Plan unless it expressly identifies the provision being modified and states that the modification is intentional.

Company shall perform the Services in a professional and workmanlike manner consistent with generally accepted managed-services industry practices. No service level, response time, resolution time, security outcome, system availability, data-recovery result, or other performance commitment shall apply unless expressly stated in this Agreement, the applicable Service Plan, or an executed Statement of Work.

1.1 Included Services. The services and features enumerated within each selected plan are deemed included as part of the Client's subscription; however, such services shall be implemented, activated, or utilized only as applicable to the Client's operational requirements. Certain features (for example, Cloud VPN Access) may remain inactive if they are not required in the Client's current environment. Should the need for any included services arise during the term of this Agreement, such services shall be made available to the Client without additional charge under the applicable plan; provided, however, that any configuration, customization project work, or other efforts necessary to integrate or enable such service within the Client's environment shall constitute billable professional services at Trinity Networx's current rates. The Client acknowledges that Trinity Networx shall have no obligation to implement or maintain any included service where the Client declines recommended changes, configurations, or integrations required for proper operation, and Trinity Networx shall bear no liability for any resulting limitation, nonperformance, or deficiency in coverage or functionality.

2. FEES; INVOICING; PAYMENT

2.1 Recurring Services. Unless an applicable Order, Service Plan, or Statement of Work expressly provides otherwise, recurring monthly fees are invoiced in advance and are due on the first day of each calendar month. Client's obligation to pay recurring fees is not contingent upon Client's receipt or use of any particular volume of Services during the applicable billing period.

2.2 Projects, Products, and Additional Services. Fees for projects, hardware, software, licenses, subscriptions, onsite services, after-hours services, usage-based services, and other nonrecurring items shall be invoiced according to the applicable Order, Statement of Work, milestone schedule, or invoice. If no specific payment schedule applies, payment is due upon receipt of the invoice.

2.3 Advance Payment. Company may require advance payment for prepaid services, recurring subscriptions, hardware, software, licenses, third-party commitments, projects, onboarding, or other Services before placing an order, reserving personnel, or beginning work. Company is not required to advance funds or extend credit on Client's behalf.

2.4 Noncancelable and Nonrefundable Charges. Fees paid or payable for activated licenses, subscriptions, cloud services, telecommunications services, ordered equipment, reserved resources, third-party commitments, and completed Services are noncancelable and nonrefundable unless the applicable Order, Statement of Work, or provider terms expressly state otherwise.

2.5 Payment Method. Client shall pay all invoices through a payment method approved by Company. If Client separately enrolls in automatic payment, Client authorizes Company to charge the designated payment method for undisputed amounts when due. Client shall maintain current billing information and promptly update any expired, replaced, or invalid payment method.

2.6 No Setoff or Deduction. Client shall pay all undisputed amounts without setoff, deduction, counterclaim, withholding, or reduction, except as required by applicable law or expressly authorized in writing by Company.

2.7 Invoice Review and Disputes. Client shall review each invoice promptly and provide Company with written notice of any good-faith dispute within ten calendar days after the invoice date. The notice must identify the disputed charge, the amount disputed, and the factual basis for the dispute in reasonable detail.

2.7.1 Undisputed Amounts. Client shall timely pay all portions of an invoice that are not disputed in good faith.

2.7.2 Good-Faith Resolution. The parties shall work in good faith to resolve a timely submitted dispute. If the disputed amount is determined to be payable, Client shall pay that amount within five Business Days after resolution.

2.7.3 Untimely Disputes. Client's failure to dispute a charge within the stated period constitutes acceptance of the invoice, except for a demonstrable billing error that Client could not reasonably have discovered during that period.

2.8 Late Payment Charge. If an undisputed amount remains unpaid for five calendar days after its due date, Company may assess a one-time administrative late charge equal to the lesser of $150.00 or five percent of the overdue amount. The parties agree that this charge is intended to compensate Company for the administrative and operational costs associated with delinquent payment and is not intended as a penalty.

2.9 Interest on Past-Due Amounts. In addition to the administrative late charge, an undisputed balance remaining unpaid for thirty calendar days after its due date may accrue interest at the lesser of one percent per month or the maximum rate permitted by applicable law. Interest shall accrue from the thirty-first calendar day until the balance is paid.

2.10 Returned or Rejected Payments. Client shall reimburse Company for reasonable bank charges, payment-processor charges, returned-payment fees, and other direct costs caused by a rejected, reversed, dishonored, or unsuccessful payment. Company may require future payments by electronic funds transfer, wire transfer, cashier's check, or another secured method after a payment is rejected or reversed.

2.11 Material Payment Default. Client's failure to pay an undisputed amount within ten calendar days after its due date constitutes a material breach of this Agreement. Company may suspend or terminate affected Services as provided in Section 9.4 after providing the notice and cure opportunity required by that Section.

2.12 Suspension and Reactivation. Suspension of Services does not waive Client's payment obligations, extend the Agreement's term, or relieve Client from charges that continue during the suspension, including recurring fees and noncancelable third-party commitments. Before restoring suspended Services, Company may require payment of all past-due amounts, applicable late charges, interest, collection costs, reconnection charges, and a reasonable advance deposit.

2.13 Taxes and Governmental Charges. Fees do not include sales, use, excise, telecommunications, regulatory, value-added, or similar taxes, fees, assessments, or governmental charges. Client shall pay all such amounts arising from the Services or products furnished to Client, excluding taxes based upon Company's net income. If Client claims a tax exemption, Client shall provide valid exemption documentation before the applicable charge is invoiced.

2.14 Changes in Service Quantities. Fees based on users, devices, locations, servers, licenses, storage, usage, or other quantities may be adjusted to reflect the quantities actually deployed, assigned, activated, or supported during the billing period, subject to any minimum commitment. Unless otherwise stated in an Order, additions may be prorated for the remaining portion of the billing period, while reductions take effect at the beginning of the next billing period after Company processes the authorized reduction.

2.15 Collection Costs and Attorneys' Fees. Client shall reimburse Company for reasonable collection-agency fees, filing fees, service fees, court costs, and other reasonable out-of-pocket expenses incurred to collect an undisputed past-due balance. If either party brings an action to enforce this Agreement, the prevailing party may recover its reasonable attorneys' fees and costs to the extent permitted by applicable law.

2.16 Application of Payments. Company may apply payments first to collection costs, returned-payment charges, late charges, and accrued interest, and then to the oldest outstanding principal balance, unless applicable law requires a different application.

2.17 Time Is of the Essence. Time is of the essence with respect to Client's payment obligations under this Agreement, each Service Plan, Order, and Statement of Work.

3. AUTHORIZED CONTACTS AND CLIENT APPROVALS

3.1 Designation of Authorized Contacts. Client shall designate one or more individuals, each an “Authorized Contact,” to communicate with Company and provide instructions concerning the Services. Client’s initial Authorized Contact is:

##CustomerFirstName## ##CustomerLastName##, ##CustomerTitle##

Client may designate different Authorized Contacts for particular Service Plans, Orders, Statements of Work, projects, locations, departments, billing matters, security matters, or other specified purposes.

3.2 Scope of Authority. Subject to any written limitations provided to Company, each Authorized Contact has authority on Client’s behalf to:

3.2.1 Service Direction. Request, prioritize, schedule, modify, approve, suspend, or cancel Services and provide operational direction concerning Client’s covered environment;

3.2.2 Statements of Work and Change Orders. Review, approve, and execute Statements of Work, Change Orders, project authorizations, and other service documents;

3.2.3 Purchases and Charges. Approve purchases, licenses, subscriptions, equipment, projects, hourly services, after-hours work, and other charges;

3.2.4 Access and Security. Authorize user access, account creation or removal, permissions, security changes, data access, credential resets, and modifications to Client’s systems;

3.2.5 Third-Party Providers. Authorize Company to communicate and coordinate with Client’s vendors, insurers, consultants, legal counsel, accountants, and other third parties; and

3.2.6 Client Decisions. Make other decisions and provide information, approvals, consents, and instructions reasonably necessary for Company to perform the Services.

3.3 Limitations on Authority. Client may establish written limits on an Authorized Contact’s authority, including financial approval limits, authorized locations, permitted systems, types of requests, or applicable Statements of Work. A limitation is not effective against Company until Company receives and has a reasonable opportunity to process written notice of that limitation.

3.4 Company’s Right to Rely. Company may rely upon the identity, instructions, approvals, representations, and apparent authority of an Authorized Contact without independently verifying the Authorized Contact’s internal authority for each request. Client is responsible for all actions Company reasonably takes in reliance upon an Authorized Contact’s instructions before Company receives and processes written notice that the person’s authority has been revoked or limited.

3.5 Verification of Sensitive Requests. Company may require additional identity verification, written confirmation, multifactor authentication, executive approval, or another security procedure before acting upon a request involving sensitive data, privileged access, financial transactions, payment instructions, ownership disputes, major system changes, security controls, account recovery, or another elevated-risk activity. Company may delay or decline a request that cannot be reasonably verified without being considered in breach of this Agreement.

3.6 Changes to Authorized Contacts. Client may add or remove an Authorized Contact or modify an Authorized Contact’s information or authority by providing Company with written notice. The notice must include the applicable person’s name, title, business address, email address, telephone number, scope of authority, and any financial or operational limitations.

3.7 Effective Time of Changes. A change to an Authorized Contact becomes effective after Company receives the written notice, reasonably verifies the request, and updates its applicable records. Company shall not be responsible for actions taken in reasonable reliance on prior authorization before completing that process.

3.8 Client's Duty to Maintain Current Information. Client shall promptly notify Company when an Authorized Contact separates from Client, changes positions, loses authority, changes contact information, or no longer requires access. Client's failure to maintain accurate Authorized Contact information does not invalidate actions Company previously took in reasonable reliance on its records.

3.9 Conflicting Instructions. If Company receives conflicting, inconsistent, or disputed instructions from Authorized Contacts, Company may suspend the affected work until Client's chief executive, owner, or another person with superior documented authority resolves the conflict in writing. Company shall receive a reasonable extension of any affected deadline and may charge for additional work resulting from the conflict.

3.10 Emergency Protective Action. Nothing in this Section prevents Company from taking reasonable temporary action without prior approval when Company reasonably believes immediate action is necessary to protect Client, Company, a third party, data, systems, or Services from an active cybersecurity threat, material service failure, unlawful activity, or imminent harm. Company shall notify an Authorized Contact as soon as reasonably practicable after taking such action.

3.11 Separate Project Contacts. An Authorized Contact designated only for a particular Statement of Work, project, location, or department has authority limited to that designated scope unless Client expressly provides broader authority in writing.

3.12 No Authority Over Company. An Authorized Contact may direct and approve Services on Client's behalf but has no authority to control Company's personnel, employment decisions, internal procedures, security methods, subcontractors, or manner and means of performing the Services.

4. ACCESS TO PREMISES, LOCATIONS, AND SYSTEMS

4.1 Access Authorization. To the extent Company performs Services at Client's offices, facilities, jobsites, warehouses, temporary locations, or other property controlled by Client, collectively, the "Premises," Client grants Company and its authorized personnel and subcontractors a limited, nonexclusive, revocable license to enter and exit the Premises and access the areas reasonably necessary to perform the Services. This authorization does not create a leasehold, tenancy, easement, or other property interest in favor of Company.

4.2 Access to Other Locations. If Services will be performed at a location not owned or controlled by Client, Client shall, at its own expense and before the Services begin, obtain all rights of entry, owner approvals, tenant approvals, site authorizations, licenses, permits, escorts, security clearances, and other permissions necessary for Company to enter the location and perform the Services.

4.3 Physical and Electronic Access. Client shall provide Company with timely physical, remote, virtual, administrative, and cloud-based access reasonably necessary to perform the Services. Required access may include:

4.3.1 Premises and Work Areas. Access to offices, jobsites, telecommunications rooms, server rooms, equipment rooms, ceilings, risers, utility areas, workspaces, and other authorized areas;

4.3.2 Covered Technology. Access to covered computers, servers, networks, firewalls, switches, wireless systems, applications, databases, cloud environments, communication platforms, backup systems, and other covered technology;

4.3.3 Credentials and Authentication. Administrative accounts, passwords, authentication approvals, recovery codes, encryption keys, security tokens, certificates, service accounts, and other access methods;

4.3.4 Keys and Access Devices. Physical keys, access cards, entry codes, alarm instructions, lockbox information, and other physical access devices; and

4.3.5 Client Personnel and Vendors. Reasonable access to Client personnel, Authorized Contacts, property managers, contractors, vendors, and other persons whose information, approval, or cooperation is necessary to perform the Services.

4.4 Least-Privilege Access. Company's access shall be limited to the systems, data, locations, permissions, and resources reasonably necessary to perform the authorized Services. Company may maintain administrative, emergency, monitoring, backup, or security access when reasonably necessary to manage, protect, support, or recover the covered environment.

4.5 Client Access Responsibilities. Client shall:

4.5.1 Timely Access. Ensure that Company can access the applicable Premises, systems, equipment, and personnel at the scheduled time;

4.5.2 Accurate Information. Provide accurate site information, access instructions, system information, credentials, documentation, and points of contact;

4.5.3 Legal Authority. Confirm that Client possesses the legal and contractual authority to grant the required access;

4.5.4 Site Coordination. Coordinate access with landlords, property managers, general contractors, subcontractors, security personnel, and other controlling parties;

4.5.5 Work Area Preparation. Provide a reasonably safe, accessible, adequately lighted, and suitable work area with necessary electrical power, environmental controls, and connectivity; and

4.5.6 Notice of Restrictions. Notify Company in advance of access restrictions, security procedures, hazardous conditions, required training, union requirements, site rules, operating-hour limitations, or other circumstances that may affect the Services.

4.6 Company Compliance With Site Rules. Company shall use commercially reasonable efforts to comply with lawful and reasonable safety, security, confidentiality, and access rules that Client provides to Company in writing before Company enters the applicable location. Company is not bound by a site rule that materially changes the scope, cost, risk, or timing of the Services unless Company accepts that change in writing.

4.7 Safety and Hazardous Conditions. Company may delay, suspend, or stop work if Company reasonably determines that a location or condition presents a safety hazard, unlawful condition, undisclosed environmental risk, or unreasonable danger to personnel, equipment, property, or systems. Company shall notify an Authorized Contact and may resume work after the condition has been corrected or the parties agree upon appropriate protective measures.

4.8 Construction and Jobsite Conditions. For Services performed at an active construction site, Client shall coordinate Company's access with the property owner, general contractor, construction manager, and applicable trades. Client shall disclose applicable safety requirements and identify areas in which Company's work may interfere with or depend upon other construction activities. Unless expressly included in a Statement of Work, Company is not responsible for site control, construction sequencing, trade coordination, temporary power, structural work, hazardous-material abatement, or correction of another contractor's work.

4.9 Credential and Key Protection. Company shall use commercially reasonable safeguards to protect Client-provided credentials, keys, access cards, codes, and authentication materials within Company's possession or control. Client shall transmit sensitive access information through Company's approved secure method and shall not require Company personnel to share individual Company credentials.

4.10 Access to Company-Owned Equipment. Client shall not relocate, disconnect, modify, access, conceal, encumber, sell, or interfere with Company-Owned Equipment without Company's prior written consent. Client shall provide Company with reasonable access to inspect, maintain, repair, replace, secure, or remove Company-Owned Equipment.

4.11 Access Delays and Restrictions. Company shall not be responsible for any delay, missed milestone, service interruption, inability to perform, or failure to meet a service level caused by Client's failure or refusal to provide timely and sufficient access. Company shall receive a reasonable extension of the affected performance period and may charge Client for resulting standby time, return visits, rescheduling, travel, expedited work, or other additional costs.

4.12 Denial or Revocation of Access. Client may temporarily restrict physical or electronic access for a legitimate security or safety reason by notifying Company as soon as reasonably practicable. If the restriction prevents Company from performing the Services, Company may suspend the affected Services until appropriate access is restored. Client remains responsible for recurring fees and noncancelable third-party charges during the suspension.

4.13 Restoration of Premises. Company shall use commercially reasonable care when performing Services at the Premises. Unless a Statement of Work expressly includes restoration, Company is not responsible for painting, patching, refinishing, ceiling repair, wall repair, landscaping, or other cosmetic restoration reasonably resulting from authorized installation, maintenance, cabling, equipment removal, or access work.

4.14 Damage Caused by Company. Subject to the limitations of liability stated in this Agreement, Company shall be responsible for direct physical damage to tangible property to the extent caused by the negligence or willful misconduct of Company or its personnel while performing Services at the Premises. Company is not responsible for ordinary wear and tear, preexisting conditions, concealed conditions, defective construction, or damage caused by Client or another person.

5. SERVICE COVERAGE; SUPPORT REQUESTS; BILLABLE SERVICES

5.1 Normal Business Hours. Unless an applicable Service Plan, Order, or Statement of Work expressly provides otherwise, Company's normal business hours are 8:00 a.m. through 5:00 p.m. Pacific Time, Monday through Friday, excluding Company-recognized holidays, collectively, "Normal Business Hours."

5.2 Business-Hours Service Coverage. Remote support and scheduled onsite Services shall be performed during Normal Business Hours, subject to the scope, reasonable-use limitations, exclusions, and response commitments of Client's selected Service Plan. Onsite Services are included only when expressly identified in the applicable Service Plan, Order, or Statement of Work.

5.3 Plan-Specific Support Coverage. Support coverage is determined by Client's applicable Service Plan.

5.3.1 Trinity Foundation. Trinity Foundation is a co-managed service plan and does not include unlimited direct end-user help desk support. Company provides escalation-level support to Client's qualified internal information technology personnel, subject to Exhibit 1.

5.3.2 Trinity Complete. Trinity Complete includes reasonable-use remote help desk support for covered users during Normal Business Hours, subject to Exhibit 2.

5.3.3 Trinity Complete Secure. Trinity Complete Secure includes reasonable-use remote help desk support for covered users during Normal Business Hours and the enhanced monitoring and cybersecurity services identified in Exhibit 3.

SUPPORT REQUESTS AND ESCALATION

5.4 Support Request Channels. Client and its covered users shall submit support requests through one of Company's approved support channels.

5.4.1 Email. By email to Company's designated help desk address.

5.4.2 Telephone. By telephone to Company's designated support number, particularly when email is unavailable or the issue is urgent.

5.4.3 Client Portal. Through Company's designated client-support portal.

5.4.4 Approved Chat. Through a direct-chat platform approved and monitored by Company.

Company may add, remove, or modify support channels upon reasonable notice, provided Client continues to have a commercially reasonable method of requesting support.

5.5 Trouble Tickets Required. Each support request shall be recorded as a trouble ticket, incident, service request, or other tracked record, collectively, a “Trouble Ticket,” and assigned a reference number when supported by Company’s system. Company is not required to begin work, measure a response time, or apply a service-level commitment until a Trouble Ticket has been created.

5.5.1 Telephone and Chat Requests. A telephone call, voicemail, text message, or chat communication does not eliminate the Trouble Ticket requirement. Company may create the Trouble Ticket on Client’s behalf based on the information provided.

5.5.2 Monitoring and Emergency Exception. Company may create and act upon a Trouble Ticket generated through automated monitoring or an urgent security event without waiting for Client to submit a separate request.

5.6 Required Ticket Information. Client shall provide the information reasonably necessary for Company to evaluate and address the request, including the affected user, device, system, location, error message, business impact, urgency, relevant screenshots, recent changes, and troubleshooting already performed. Incomplete or inaccurate information may delay classification and response.

5.7 Ticket Priority and Classification. Company shall assign each Trouble Ticket a priority based on the information reasonably available to Company, including the number of affected users, business impact, security risk, availability of a workaround, and scope of the interruption. Client’s characterization of an issue as urgent does not control its final priority classification.

5.7.1 Priority Reclassification. Company may raise or lower a Trouble Ticket’s priority as additional information becomes available or the effect of the issue changes.

5.7.2 Multiple Issues. Company may separate unrelated issues submitted in a single request into multiple Trouble Tickets and prioritize each issue independently.

5.8 Support Response Times. Company shall use commercially reasonable efforts to respond to Trouble Tickets according to the response targets stated in the applicable Service Plan, Order, Statement of Work, or Support Response Time Schedule.

5.8.1 Response Defined. A “response” means Company’s acknowledgment of the request, initial communication with Client, or commencement of initial triage. A response target is not a guaranteed resolution time.

5.8.2 Measurement Period. Unless expressly stated otherwise, response times are measured only during the service hours applicable to Client’s Service Plan. Time outside the applicable service period does not count toward a business-hours response target.

5.8.3 Response Dependencies. Response and resolution may be delayed by Client’s availability, incomplete information, restricted access, third-party providers, hardware availability, vendor support, internet or utility failures, security conditions, or other circumstances outside Company’s reasonable control.

5.9 Escalation. Company shall escalate Trouble Tickets through its internal support levels based on priority, technical complexity, business impact, security risk, personnel availability, and the need for specialized or third-party assistance.

5.9.1 Client Escalation Requests. An Authorized Contact may request escalation by identifying the Trouble Ticket and explaining the material business or security impact requiring additional attention.

5.9.2 Vendor Escalation. Company may coordinate with an applicable third-party provider when reasonably necessary. Vendor coordination does not make Company responsible for the provider's response time, performance, charges, or resolution.

5.10 Ticket Closure. Company may close a Trouble Ticket after completing the requested work, providing a reasonable resolution or workaround, determining that the issue is outside scope, referring the matter to an appropriate third party, or making reasonable attempts to obtain required information or confirmation from Client without receiving a response. A recurring or unresolved issue may be reopened or submitted as a new Trouble Ticket, depending on the circumstances.

MONITORING AND DIAGNOSTICS

5.11 Continuous Automated Monitoring. When included in Client's Service Plan, Company shall provide automated monitoring and diagnostic services twenty-four hours per day, seven days per week, throughout the year, subject to maintenance, third-party availability, technical limitations, and the exclusions stated in this Agreement.

5.11.1 Automated Monitoring Distinguished. "24/7 monitoring," "continuous monitoring," "proactive monitoring," and similar descriptions refer primarily to automated tools that collect information, evaluate configured conditions, and generate alerts. Such descriptions do not mean Company continuously staffs Client's environment or provides unlimited human investigation, remediation, end-user support, or onsite response at all hours.

5.11.2 Alert Review and Response. Company shall review and respond to monitoring alerts according to their assigned severity, Client's Service Plan, the applicable service period, and Company's operating procedures. Human response outside Normal Business Hours may be separately chargeable unless expressly included in Client's Service Plan.

HOURLY AND AFTER-HOURS SERVICES

5.12 After-Hours Support. Services requested or performed outside Normal Business Hours are provided on a commercially reasonable, best-efforts basis unless an applicable Service Plan or Statement of Work expressly provides dedicated after-hours coverage.

5.12.1 No Guaranteed Availability. Company does not guarantee that personnel, specialized expertise, replacement equipment, vendors, or onsite support will be available outside Normal Business Hours.

5.12.2 Authorization. Company may require authorization from an Authorized Contact before beginning separately billable after-hours work. If immediate action is reasonably necessary to prevent material harm, contain an active security threat, or protect systems or data, Company may take proportionate protective action under Section 3.10.

5.13 Agreement-Client Rates. Clients with an active Service Plan shall receive the following discounted hourly rates for Services not included in their recurring fees.

Time of Service	Agreement Client Rate	Minimum Charge
Normal Business Hours, Monday through Friday, 8:00 a.m. to 5:00 p.m.	$235.00 per hour	As stated in the applicable Order or Statement of Work
Weekday After-Hours, Monday through Friday, 5:00 p.m. to 8:00 a.m.	$470.00 per hour	Two hours
Weekends, from 12:01 a.m. Saturday through 8:00 a.m. Monday	$705.00 per hour	Three hours

Time of Service	Agreement Client Rate	Minimum Charge
Company-Recognized Holidays	$705.00 per hour	Three hours

5.14 Non-Agreement Client Rates. Clients without an active Service Plan shall be billed at the following hourly rates.

Time of Service	Non-Agreement Client Rate	Minimum Charge
Normal Business Hours, Monday through Friday, 8:00 a.m. to 5:00 p.m.	$345.00 per hour	As stated in the applicable quote or work authorization
Weekday After-Hours, Monday through Friday, 5:00 p.m. to 8:00 a.m.	$690.00 per hour	Two hours
Weekends, from 12:01 a.m. Saturday through 8:00 a.m. Monday	$1,035.00 per hour	Three hours
Company-Recognized Holidays	$1,035.00 per hour	Three hours

5.15 Application of Premium Rates. The applicable hourly rate is determined by when the Services are performed, regardless of whether the Services are performed remotely or onsite. Weekend and holiday rates apply regardless of the time of day and do not combine with the weekday after-hours multiplier. If more than one premium-rate category applies, only the highest applicable rate shall be charged.

5.16 Minimum Charges. The applicable minimum charge applies to each separately requested or dispatched after-hours service event. Time exceeding the minimum shall be billed according to Company's then-current billing increments. Travel time, mileage, parking, lodging, shipping, and other expenses may be separately charged when applicable.

5.17 Company-Recognized Holidays. Unless Company provides a revised holiday schedule, Company-recognized holidays are:

5.17.1 New Year's Day;

5.17.2 Memorial Day;

5.17.3 Independence Day;

5.17.4 Labor Day;

5.17.5 Thanksgiving Day and the immediately following Friday;

5.17.6 Christmas Eve; and

5.17.7 Christmas Day.

If a listed holiday is officially observed by Company on a different weekday, the observed day shall be treated as the holiday for purposes of service availability and billing.

5.18 Client-Specific Operating Hours. Company shall use commercially reasonable efforts to coordinate scheduled work with Client's business operations. Work requested outside Normal Business Hours, during restricted operating periods, or on an expedited basis may be subject to premium rates, scheduling charges, travel charges, or other additional fees.

5.19 Onsite Services. Onsite Services must be scheduled through Company and are subject to personnel availability, geographic coverage, travel requirements, site access, and Section 4. Unless expressly included in

Client’s Service Plan or Statement of Work, onsite labor, travel time, mileage, parking, lodging, and related expenses are separately billable.

OUT-OF-SCOPE SERVICES AND COSTS

5.20 Out-of-Scope Services. Any service not expressly included in Client’s applicable Service Plan, Order, or Statement of Work is outside scope and separately billable at the applicable rate stated in this Section or under a separate quote or Statement of Work.

5.20.1 Hardware and Equipment. Computers, servers, firewalls, switches, wireless equipment, peripherals, replacement parts, accessories, and other hardware are not included unless expressly stated.

5.20.2 Software and Licensing. Software, licenses, subscriptions, cloud services, security tools, backup services, warranties, support agreements, and other third-party charges are not included unless expressly stated.

5.20.3 Projects and Changes. Projects, migrations, installations, upgrades, relocations, new-location deployments, major configuration changes, integration work, and remediation are not included unless expressly stated.

5.20.4 Specialized Services. Digital forensics, incident response, penetration testing, compliance work, database repair, application development, structured cabling, and other specialized services are not included unless expressly stated.

5.20.5 Excessive or Nonstandard Support. Services exceeding the applicable reasonable-use limitation, repeated work caused by Client’s failure to follow recommendations, or work involving unsupported or nonstandard technology may be treated as out of scope.

5.21 Authorization of Out-of-Scope Work. Company may require approval from an Authorized Contact before performing out-of-scope work. Client’s request for, approval of, or knowing acceptance of out-of-scope work constitutes authorization to invoice the work at the applicable rate.

USER, DEVICE, SUBSCRIPTION, AND LICENSE COUNTS

5.22 Periodic Environment Reconciliation. Company may periodically use its remote monitoring, security, licensing, cloud-management, or other administrative tools to inventory covered users, devices, subscriptions, licenses, locations, servers, storage, and other billable quantities, collectively, “Service Quantities.”

5.23 Increases in Service Quantities. Company may increase Client’s billed Service Quantities when additional users, devices, subscriptions, licenses, or other billable items are requested, assigned, activated, deployed, detected, or supported.

5.23.1 Effective Date. An increase may become effective as of the date the additional Service Quantity is activated, deployed, or first supported and may be prorated for the remaining billing period.

5.23.2 Client Responsibility. Client is responsible for charges associated with additions requested or authorized by an Authorized Contact and for additions created through Client’s hiring, deployment, licensing, or operational decisions.

5.24 Reductions in Service Quantities. Client is responsible for notifying Company when a user, device, subscription, license, or other billable item is no longer required. Reduction requests must be submitted to **help@trinitynetworx.com** or through another support channel designated by Company.

5.24.1 Processing Date. A valid reduction request received on or before the fifteenth day of a calendar month may take effect in the next billing cycle. A request received after the fifteenth may take effect in the following billing cycle.

5.24.2 No Retroactive Credits. Company is not required to issue a retroactive credit for a user, device, license, subscription, or other Service Quantity that remained deployed, assigned, available, or recorded as active before Company received and processed the reduction request.

5.24.3 Minimum Commitments. A reduction does not reduce fees below an applicable minimum user count, monthly commitment, contractual quantity, or noncancelable third-party commitment.

5.24.4 Provider Restrictions. Reductions remain subject to applicable third-party provider restrictions, commitment periods, cancellation windows, and renewal requirements.

ACCOUNT AND SERVICE REVIEWS

5.25 Quarterly Account Review. Company may conduct an account and service review quarterly or at another reasonable interval based on Client's applicable Service Plan and operational requirements. The review may evaluate:

5.25.1 Service Activity. Trouble Ticket volume, ticket priority, support hours, escalation activity, and recurring issues;

5.25.2 Environment Size. Users, devices, servers, locations, subscriptions, licenses, storage, networks, and supported systems;

5.25.3 Service Complexity. Onboarding, offboarding, application support, vendor coordination, security requirements, documentation, and administrative processes;

5.25.4 Onsite and After-Hours Usage. Scheduled and unscheduled onsite visits, emergency requests, after-hours work, and travel requirements; and

5.25.5 Risk and Service Alignment. Security risk, unsupported technology, compliance requirements, changes in Client's operations, and whether the current Service Plan remains appropriate.

5.26 Service and Pricing Adjustments. Company may correct billing errors and adjust fees to reflect actual Service Quantities under Sections 5.22 through 5.24. If an account review identifies a material change in scope, complexity, risk, support demand, or service-delivery cost, Company may propose changes to the Service Plan, scope, minimum commitment, or pricing.

A material change to recurring rates or the fundamental scope of the Service Plan shall be provided in writing and shall become effective only as permitted by the applicable Order, renewal terms, or amendment provisions of this Agreement. Until the parties agree upon a material scope change, Company may treat excess or nonstandard services as out-of-scope work or exercise its other rights under this Agreement.

NONSTANDARD USER ADMINISTRATION

5.27 Nonstandard or Complex Environments. A Client environment may be classified as nonstandard or complex when user administration requires materially greater effort than Company's standard process. Relevant conditions may include:

5.27.1 Detailed Onboarding Requirements. Multiple approval levels, customized access matrices, numerous applications, specialized devices, extensive data migration, or department-specific configurations;

5.27.2 Detailed Offboarding Requirements. Legal holds, extensive data transfer, equipment retrieval, multi-platform access removal, mailbox conversion, or specialized retention requirements;

5.27.3 Specialized Applications. Client-specific line-of-business, construction-management, accounting, database, security, or third-party applications requiring nonstandard administration;

5.27.4 Multiple Locations or Entities. User administration involving multiple companies, tenants, domains, jobsites, business units, or regulatory environments; or

5.27.5 Client-Specific Procedures. Detailed documentation, unusual scheduling, expedited processing, manual reporting, or other requirements outside Company's standard workflow.

5.28 Included Onboarding and Offboarding Allowance.

5.28.1 Trinity Foundation. Trinity Foundation does not include routine end-user onboarding or offboarding unless expressly stated in an Order or Statement of Work.

5.28.2 Trinity Complete and Trinity Complete Secure. Trinity Complete and Trinity Complete Secure include up to two standard onboarding events and two standard offboarding events during each calendar month unless the applicable Order states otherwise.

5.28.3 No Accumulation. Unused onboarding or offboarding events do not carry forward to a later month and have no cash or credit value.

5.29 Additional Onboarding and Offboarding Charges. Unless the applicable Order states otherwise, events exceeding the monthly allowance shall be billed as follows:

Service Event	Additional Charge
Additional standard onboarding	$650.00 per user
Additional standard offboarding	$300.00 per user

5.29.1 Nonstandard Work. Equipment procurement, workstation imaging, data migration, application consulting, physical equipment retrieval, shipping, onsite services, after-hours work, legal holds, forensic preservation, and other nonstandard requirements are separately billable in addition to the event fee.

5.29.2 Rate Changes. Company may propose changes to onboarding and offboarding rates according to the amendment, renewal, or pricing-adjustment provisions of this Agreement. A posted or uncommunicated rate change does not retroactively alter an executed Order.

MICROSOFT NEW COMMERCE EXPERIENCE SUBSCRIPTIONS

5.30 Application of Microsoft NCE Terms. This Section applies to Microsoft license-based products purchased, renewed, migrated, or administered by Company through Microsoft's New Commerce Experience or a successor program, collectively, "Microsoft NCE Subscriptions."

5.31 Subscription Term and Billing Frequency. Each Microsoft NCE Subscription is subject to the commitment term, billing frequency, license quantity, product, renewal setting, and pricing identified in the applicable Order or provider record. A monthly billing frequency does not mean the subscription has a month-to-month commitment.

5.32 Limited Cancellation and Reduction Window. Client acknowledges that Microsoft generally permits cancellation or license-quantity reduction only during a limited period following the initial purchase, renewal, or addition of licenses. After the applicable provider window closes, the subscription and committed quantity generally cannot be canceled or reduced until the next renewal date.

5.32.1 Client Instructions. Client shall submit any requested cancellation or reduction to Company sufficiently in advance to allow Company to process it within Microsoft's applicable deadline.

5.32.2 No Guaranteed Processing. Company does not guarantee that Microsoft will accept a cancellation, reduction, or change. A request is effective only after Microsoft or the applicable distributor confirms the change.

5.33 License Increases. Client may request additional licenses during a subscription term. Any additional licenses may become subject to Microsoft's commitment and cancellation rules and may remain billable through the applicable subscription expiration or renewal date.

5.34 Renewal. Unless the applicable Order states otherwise, Microsoft NCE Subscriptions are configured to renew automatically for a term corresponding to the existing subscription.

5.34.1 Notice of Nonrenewal. Client must provide Company with written notice of cancellation, nonrenewal, or requested quantity reduction at least forty-five days before the applicable renewal date.

5.34.2 Untimely Notice. If Client fails to provide timely notice and the subscription renews, Client remains responsible for all charges during the renewed commitment term.

5.34.3 Scheduled Changes. When supported by Microsoft, Company may schedule an approved cancellation, quantity reduction, product change, or billing change to take effect at renewal.

5.35 Effect of Agreement Termination. Termination of this Agreement does not cancel or eliminate Client's payment responsibility for an active Microsoft NCE Subscription or other noncancelable provider commitment.

5.35.1 Continued Payment. Client may remain responsible for monthly payments through the end of the Microsoft commitment term, including through authorized automated clearing house withdrawals or another payment method approved by Company.

5.35.2 Transfer or Purchase of Remaining Commitment. If Microsoft, the distributor, and Company permit, Client may assume, transfer, or purchase the remaining subscription commitment according to the applicable provider procedures. Company does not guarantee that a transfer will be available.

5.35.3 Accelerated Payment. If Client fails to maintain an approved payment method or creates a material risk that Company will remain liable for the subscription, Company may require advance payment of the remaining committed charges to the extent permitted by the applicable Order and law.

5.36 Microsoft Changes. Microsoft or its distributor may change products, pricing, features, licensing models, renewal procedures, cancellation rights, service availability, or other provider terms. Client is responsible for applicable pass-through changes according to Section 18 and the applicable Order.

5.37 Microsoft Service and Data Consequences. Cancellation, expiration, suspension, or nonrenewal of a Microsoft NCE Subscription may result in loss of access, reduced functionality, or eventual deletion of data according to Microsoft's then-current policies. Client is responsible for arranging replacement licensing and exporting required data before service access expires.

THIRD-PARTY HARDWARE

5.38 Hardware Not Purchased Through Company. Hardware purchased or obtained from another vendor and proposed for introduction into Client's covered environment is not automatically included in the Services.

5.38.1 Compatibility and Security Assessment. Company may require an assessment before connecting, configuring, supporting, or managing the hardware. Assessment, installation, configuration, integration, remediation, and onsite work are separately billable at the applicable rates.

5.38.2 No Compatibility Guarantee. Company does not warrant that outside-purchased hardware will be compatible with Client's environment, meet Company's supported-technology standards, satisfy security requirements, or operate as represented by the seller.

5.38.3 Vendor and Warranty Responsibility. Client is responsible for returns, exchanges, warranties, licensing, support, and claims involving hardware not purchased through Company. Company may assist with the outside vendor on a separately billable basis.

5.38.4 Right to Decline Support. Company may decline to connect, manage, or support hardware that is obsolete, unsupported, insecure, improperly licensed, counterfeit, incompatible, or otherwise presents an unreasonable operational or security risk.

MOBILE-DEVICE SUPPORT

5.39 Included Mobile Email Configuration. Unless the applicable Service Plan or Order states otherwise, Company will provide reasonable remote assistance with configuring Company-supported business email on one supported mobile device per covered user.

5.39.1 Limited Scope. Included assistance is limited to configuring the supported email account, supported authentication method, and related Company-managed security requirements.

5.39.2 Excluded Mobile Support. The following are not included unless expressly stated:

5.39.2.1 Personal applications, personal data, photographs, media, or consumer cloud services;

5.39.2.2 Device repair, replacement, warranty service, carrier support, cellular service, or hardware troubleshooting;

5.39.2.3 Data transfer, backup, recovery, or restoration of a personal device;

5.39.2.4 Support for jailbroken, rooted, obsolete, unsupported, or insecure devices;

5.39.2.5 Setup, configuration, or troubleshooting of applications other than the supported business email application; and

5.39.2.6 Onsite, after-hours, or expedited mobile-device support.

5.39.3 Mobile Device Management. Enrollment, administration, security enforcement, application deployment, remote wipe, compliance management, or other mobile-device-management services are included only when expressly stated in the applicable Service Plan or Order and properly licensed.

5.39.4 User Authorization and Data Risk. Client is responsible for obtaining appropriate user authorization before Company manages or remotely wipes a mobile device. Client and the applicable user are responsible for backing up personal data before Company performs work that may affect the device.

6. WARRANTIES; LIMITATIONS OF LIABILITY.

Any third-party products provided to Client pursuant to this Agreement, including but not limited to third-party hardware, software, peripherals, and accessories (collectively, "Third Party Products") shall be provided to Client "as is". Company shall use reasonable efforts to assign all warranties (if any) for the Third-Party Products to Client but will have no liability whatsoever for such third-party products. All Third-Party Products are provided WITHOUT ANY WARRANTY WHATSOEVER as between Company and Client, and Company shall not be held liable as an insurer or guarantor of the performance or quality of Third-Party Products.

6.1 Equipment and Software Failures. Except as expressly provided in this Section, Company shall not be liable for any failure, malfunction, interruption, degradation, incompatibility, or loss involving hardware, software, networks, telecommunications services, cloud services, or other technology, or for any loss or damage resulting from such failure. This limitation does not apply to equipment owned and provided by Company under this Agreement ("Company-Provided Equipment"). If Company-Provided Equipment fails during the term of this Agreement, Company shall, at its discretion, repair or replace the affected equipment within thirty (30) days after receiving notice of the failure, subject to equipment availability and reasonable access to Client's premises and systems.

6.2 Lawful Use of Covered Systems and Services. Client represents and warrants that Client shall not access or use any equipment, software, network, cloud service, account, platform, or other technology furnished, supported, or managed by Company under this Agreement for any purpose or activity that violates applicable law or regulation, including transmitting unsolicited bulk commercial email commonly referred to as "spam."

6.3 Exclusion of Certain Damages; Limitation of Aggregate Liability.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF REVENUE, PROFITS, SAVINGS,

BUSINESS OPPORTUNITY, GOODWILL, USE, OR DATA, ARISING OUT OF OR RELATING TO THIS AGREEMENT, ANY STATEMENT OF WORK, THE SERVICES, ANY PRODUCTS OR EQUIPMENT PROVIDED, ANY DELAY OR FAILURE IN PROVIDING THE SERVICES, OR ANY INTERRUPTION, CORRUPTION, LOSS, OR UNAVAILABILITY OF DATA, TECHNOLOGY, SYSTEMS, OR SERVICES, REGARDLESS OF THE LEGAL THEORY ASSERTED AND EVEN IF THE PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

EXCEPT FOR CLIENT'S PAYMENT OBLIGATIONS AND ANY LIABILITY THAT CANNOT LAWFULLY BE LIMITED OR EXCLUDED, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT, ALL STATEMENTS OF WORK, AND THE SERVICES, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL NOT EXCEED THE ACTUAL DIRECT DAMAGES INCURRED OR THE TOTAL FEES PAID BY CLIENT TO COMPANY FOR THE SERVICES DURING THE THREE MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM, WHICHEVER IS LESS. AMOUNTS PAID FOR HARDWARE, SOFTWARE, LICENSES, SUBSCRIPTIONS, CLOUD SERVICES, TELECOMMUNICATIONS, TAXES, SHIPPING, AND OTHER THIRD-PARTY OR PASS-THROUGH PRODUCTS AND SERVICES SHALL NOT BE INCLUDED WHEN CALCULATING THIS LIMITATION.

THE LIMITATIONS IN THIS SECTION SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW, NOTWITHSTANDING THE FAILURE OF ANY LIMITED REMEDY TO ACCOMPLISH ITS ESSENTIAL PURPOSE. NOTHING IN THIS SECTION SHALL EXCLUDE OR LIMIT LIABILITY FOR FRAUD, WILLFUL INJURY, OR ANY OTHER LIABILITY THAT MAY NOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

7. INDEMNIFICATION

7.1 General Indemnification. Each party, when acting as the "Indemnifying Party," shall indemnify, defend, and hold harmless the other party and its officers, directors, members, managers, employees, and authorized agents, collectively, the "Indemnified Parties," from and against any third-party claim, demand, action, proceeding, judgment, settlement, damage, liability, penalty, cost, or expense, including reasonable attorneys' fees and defense costs, collectively, "Losses," to the extent arising from: (a) the negligent act or omission, gross negligence, willful misconduct, or violation of applicable law by the Indemnifying Party or its employees, agents, or subcontractors; or (b) the Indemnifying Party's material breach of this Agreement that remains uncured after expiration of any applicable notice-and-cure period.

7.2 Intellectual Property Indemnification. Each party shall indemnify, defend, and hold harmless the other party's Indemnified Parties from any third-party claim alleging that materials, content, documentation, software, designs, specifications, instructions, or other work furnished by the Indemnifying Party and used as authorized under this Agreement infringe or misappropriate a third party's patent, copyright, trademark, trade secret, or other intellectual-property right. Company shall have no obligation under this Section for a claim arising from: (a) Third-Party Products; (b) materials, data, content, specifications, or instructions supplied by Client; (c) modification of a Company-provided item by anyone other than Company; (d) use of a Company-provided item in combination with a product, service, or process not supplied or approved by Company, when the claim would not otherwise have arisen; (e) use contrary to Company's documentation or instructions; or (f) Client's continued use after Company provides notice of the alleged infringement and offers a commercially reasonable replacement, modification, or discontinuation procedure.

7.3 Indemnification Procedure. An Indemnified Party seeking protection under this Section shall provide the Indemnifying Party with prompt written notice of the applicable claim. A delay in providing notice shall relieve the Indemnifying Party of its obligations only to the extent the delay materially prejudices the defense. Subject to applicable law, the Indemnifying Party may assume and control the defense using counsel reasonably acceptable to the Indemnified Party. The Indemnified Party shall provide reasonable cooperation, at the Indemnifying Party's expense, and may participate in the defense through separate counsel at its own expense. The Indemnifying Party shall not settle any claim in a manner that admits wrongdoing by an Indemnified Party, imposes liability or continuing obligations upon an Indemnified Party, or fails to provide the Indemnified Party with a complete and unconditional release, unless the affected Indemnified Party first provides written consent, which shall not be unreasonably withheld.

7.4 Allocation of Responsibility. The Indemnifying Party shall have no obligation to indemnify, defend, or hold harmless an Indemnified Party to the extent a claim or Loss resulted from the negligence, willful misconduct, violation of law, or material breach of this Agreement by that Indemnified Party or a person under its direction or control.

8. OWNERSHIP OF INTELLECTUAL PROPERTY; LIMITED LICENSES

8.1 Preexisting and Independently Developed Intellectual Property. Each party shall retain all right, title, and interest in and to the intellectual property that it owned, licensed, developed, acquired, or possessed before the Effective Date or developed independently of this Agreement without use of the other party's Confidential Information. No ownership interest is transferred except through an express written assignment signed by the party transferring the applicable rights.

8.2 Company Intellectual Property. Company retains all right, title, and interest in and to its software, scripts, tools, utilities, processes, methodologies, workflows, automations, configurations, templates, forms, policies, procedures, training materials, documentation systems, assessment methods, reports, designs, technical standards, know-how, and other proprietary materials, including all modifications, enhancements, derivative works, and improvements to those materials, collectively, "Company IP." Company IP does not include Client Data or intellectual property owned by Client.

8.3 Client Intellectual Property and Data. Client retains all right, title, and interest in and to Client's data, records, content, trademarks, business materials, plans, specifications, and other intellectual property furnished to Company by or on behalf of Client, collectively, "Client IP." Client grants Company and its authorized subcontractors a limited, nonexclusive, nontransferable, and revocable license to access, reproduce, process, modify, transmit, and otherwise use Client IP only as reasonably necessary to provide, secure, support, and administer the Services.

8.4 Client-Specific Deliverables. Unless a Statement of Work expressly provides otherwise, Company shall own all reports, diagrams, documentation, configurations, recommendations, designs, and other work product created by Company in connection with the Services, collectively, "Deliverables," excluding Client IP incorporated into those Deliverables. After Client has paid all amounts due for the applicable Deliverables, Company grants Client a nonexclusive, nontransferable, perpetual license to use the Deliverables internally for Client's own business operations. Client may provide a Deliverable to its attorneys, accountants, insurers, regulators, financing sources, and replacement technology provider when reasonably necessary for Client's legitimate business purposes, provided the recipient is informed of its confidential or proprietary nature and does not use it for the benefit of another person or business.

8.5 Operational License During the Agreement. During the term of this Agreement and subject to Client's payment and compliance obligations, Company grants Client a limited, nonexclusive, nontransferable, non-sublicensable, and revocable license to use Company IP expressly made available to Client solely as necessary to receive and use the Services. Except for the continuing license to fully paid Client-Specific Deliverables under Section 8.4, this license automatically terminates when the applicable Service or this Agreement terminates.

8.6 Restrictions on Use. Except with Company's prior written consent or as expressly permitted by applicable law, Client shall not: (a) sell, license, sublicense, publish, distribute, disclose, or commercially exploit Company IP; (b) copy Company IP except as reasonably necessary for Client's authorized internal use; (c) modify, translate, adapt, or create derivative works from Company IP; (d) reverse engineer, decompile, disassemble, or attempt to discover the source code, underlying structure, algorithms, trade secrets, or nonpublic methods embodied in Company IP; (e) remove or alter proprietary notices; (f) use Company IP to develop or assist a competing product or service; or (g) permit any third party to engage in conduct prohibited by this Section.

8.7 Modifications and Improvements. Unless otherwise stated in a signed Statement of Work, any modification, enhancement, adaptation, derivative work, recommendation, or improvement relating to Company IP shall remain Company IP, regardless of whether it was created by Company, requested by Client, or developed with Client's feedback. Client retains ownership of any Client IP contained in such materials.

8.8 Third-Party Products. Ownership and use of third-party software, hardware, documentation, cloud services, and other Third-Party Products are governed exclusively by the applicable third-party license, subscription, warranty, or other terms. Nothing in this Agreement grants either party ownership of, or rights exceeding those granted by the applicable provider in, any Third-Party Product.

8.9 Custom Development and Ownership Transfers. Any agreement that a Deliverable will constitute a "work made for hire," be assigned to Client, or become Client-owned intellectual property must be expressly stated in a written Statement of Work signed by Company. Payment for Services or Deliverables alone does not transfer ownership of Company IP.

8.10 Effect of Termination. Upon expiration or termination of the applicable Services, each party shall discontinue use of the other party's intellectual property except to the extent a continuing license is expressly granted under this Agreement. Company may remove or disable its software agents, security tools, monitoring tools, licenses, administrative access, and other Company-controlled technology. Client's right to use fully paid Client-Specific Deliverables under Section 8.4 shall survive termination, but Company's internal operating procedures, internal notes, credential-management systems, templates, security methods, and proprietary documentation are not Client-Specific Deliverables and need not be transferred to Client. Any transition, compilation, conversion, export, or documentation preparation requested by Client may be treated as a separately billable offboarding service.

9. TERMINATION; SUSPENSION; TRANSITION

9.1 Termination Without Cause. Either party may terminate this Agreement without cause by providing the other party with at least ninety days' prior written notice. Unless the parties agree otherwise in writing, termination shall become effective upon expiration of the ninety-day notice period. Client shall remain responsible for all recurring fees and other amounts accruing through the effective termination date, regardless of whether Client continues using the Services during the notice period.

9.2 Termination by Mutual Agreement. The parties may terminate this Agreement or any Statement of Work at any time by a written agreement signed by both parties. The written termination agreement shall identify the effective termination date and any applicable payment, transition, equipment, licensing, data-retention, or other continuing obligations.

9.3 Termination for Cause. Either party may terminate this Agreement or an affected Statement of Work by written notice if the other party materially breaches the applicable agreement and: (a) the breach is incapable of cure; or (b) the breaching party fails to cure the breach within ten days after receiving written notice describing the breach in reasonable detail. If the breach can be cured but reasonably requires more than ten days, the breaching party shall not be considered in default if it begins corrective action within the ten-day period, diligently continues that corrective action, and completes the cure within a commercially reasonable period acceptable to the nonbreaching party.

9.4 Nonpayment. Company may suspend affected Services or terminate this Agreement or an affected Statement of Work upon written notice if Client fails to pay an undisputed amount when due and does not cure the nonpayment within ten days after receiving written notice. Company may require payment of all past-due amounts, applicable late charges, collection costs, reconnection charges, and an advance deposit before restoring suspended Services. Suspension shall not waive Client’s payment obligations or extend the term of this Agreement.

9.5 Immediate Suspension or Termination. Company may immediately suspend affected Services and, when the circumstances reasonably require, terminate this Agreement or an affected Statement of Work upon written notice if: (a) Client uses the Services or any covered system for unlawful, fraudulent, abusive, or unauthorized activity; (b) Client’s conduct creates a material security threat or an unreasonable risk of harm to Company, Client, another customer, a third-party provider, or any covered system; (c) Client attempts to circumvent, disable, or interfere with Company’s security, monitoring, licensing, or management tools; (d) continued performance would violate applicable law, a court order, or a binding third-party restriction; or (e) an emergency condition makes continued performance unsafe or commercially unreasonable. When practicable, Company shall limit the suspension to the affected Services and restore those Services after the condition has been corrected and Client has paid any applicable remediation or reconnection charges.

9.6 Insolvency and Bankruptcy. To the extent permitted by applicable law, either party may terminate this Agreement or an affected Statement of Work if the other party ceases conducting business in the ordinary course, makes a general assignment for the benefit of creditors, becomes subject to the appointment of a receiver or similar custodian, or becomes subject to an insolvency, liquidation, or bankruptcy proceeding that is not dismissed within sixty days. Nothing in this Section authorizes termination, modification, or suspension based solely upon insolvency or the commencement of a bankruptcy proceeding when such action is prohibited by applicable bankruptcy law.

9.7 Termination of Statements of Work. Termination of one Statement of Work shall not terminate any other Statement of Work or this Agreement unless the applicable termination notice expressly states otherwise and the terminating party has a contractual right to terminate those additional agreements. Termination of this Agreement shall terminate all active Statements of Work as of the effective termination date unless the parties agree otherwise in writing.

9.8 Fees and Noncancelable Commitments. Upon termination or expiration, Client shall immediately pay all undisputed amounts accrued through the effective termination date. Client shall also remain responsible for any authorized, noncancelable third-party charges, license commitments, subscriptions, cloud services, equipment orders, financing obligations, project commitments, and early-termination charges incurred by Company on Client’s behalf. Except as expressly stated in this Agreement or required by applicable law, prepaid fees are nonrefundable.

9.9 Company-Owned Equipment. All equipment identified as owned, leased, or provided by Company shall remain Company property unless a written Order, equipment schedule, or purchase agreement expressly transfers title to Client. Upon expiration or termination, Client shall discontinue use of Company-owned equipment and provide Company or its authorized representative with reasonable access during normal business hours to remove the equipment. Unless the parties agree otherwise in writing, removal shall occur within fifteen business days after the effective termination date. Client may retain Company-owned equipment only if Company agrees in writing to the transfer and Client pays all outstanding amounts and any applicable purchase or buyout price.

9.10 Client-Owned Equipment. Termination shall not affect Client’s ownership of equipment for which title has transferred to Client and all applicable purchase, financing, licensing, and other charges have been paid.

Company may remove its software agents, licenses, credentials, configurations, security tools, monitoring tools, and other Company-controlled technology from Client-owned equipment upon termination.

9.11 Return and Export of Client Data. Upon Client's written request made before termination or within fifteen calendar days after the effective termination date, Company shall use commercially reasonable efforts to make Client Data then within Company's possession or control available to Client in the data's existing format or another commercially reasonable export format supported by the applicable system. CSV format shall be used only when appropriate for the type of data being exported. Company is not required to convert data into a format that the applicable system does not support, recreate unavailable data, or provide proprietary software, licensed applications, encryption keys owned by third parties, Company IP, or internal Company documentation.

9.12 Backup Data and Service Deactivation. Client acknowledges that termination may result in the expiration or deactivation of backup, security, cloud, software, monitoring, and other third-party services. Client is responsible for arranging replacement services and requesting any available export or restoration before the applicable service is deactivated. Company shall not intentionally destroy Client's available production data merely because Client provides notice of termination. After the effective termination date and expiration of the applicable transition period, Company may discontinue Services and delete or permit the expiration of Client Data maintained through Company-controlled or third-party systems, subject to applicable law, provider capabilities, ordinary backup-retention cycles, and any separately purchased retention service.

9.13 Data-Retention Period. Unless applicable law, a court order, a third-party provider's retention policy, or a separate written agreement requires otherwise, Company shall have no obligation to store Client Data more than fifteen calendar days after the effective termination date. After that period, Company may delete the data in the ordinary course without further notice. Data contained in archival or disaster-recovery backups may remain until overwritten or deleted according to Company's or the applicable provider's ordinary retention cycle, but Company shall have no obligation to restore or provide such data after the transition period.

9.14 Transition Assistance. At Client's written request and subject to Company's personnel availability, Company may provide reasonable transition assistance to Client or Client's replacement service provider. Transition assistance is outside the recurring Service Plan and shall be billed at Company's then-current rates. Company may require advance payment or a deposit before beginning transition work. Company is not required to provide transition assistance until Client has paid all undisputed past-due amounts or made other payment arrangements acceptable to Company.

9.15 Transition Materials and Credentials. Subject to payment of applicable charges, Company shall provide available Client-owned credentials and Client-Specific Deliverables that Company is contractually required to provide. Company is not required to disclose its internal notes, ticket procedures, security methods, automation scripts, proprietary templates, internal credential-management systems, tool configurations, personnel information, or other Company IP. Any compilation, conversion, sanitization, documentation, export, or preparation requested for transition purposes may be billed as an offboarding service.

9.16 Cooperation With Legal Process. Company may preserve, disclose, or produce information when reasonably necessary to comply with applicable law, a subpoena, a court order, or another valid legal demand. When legally permitted and reasonably practicable, Company shall notify Client before making the disclosure. Company shall not be liable for a good-faith disclosure made in response to valid legal process, subject to applicable law and Section 6.3.

9.17 Effect of Termination. Upon the effective termination date: (a) Company may discontinue the terminated Services; (b) all licenses granted solely for receipt of those Services shall terminate, except for licenses expressly stated to survive; (c) Client shall cease using Company IP and Company-controlled tools except as otherwise authorized in writing; and (d) each party shall return or destroy the other party's Confidential Information as required by this Agreement, subject to legal-retention requirements and ordinary backup practices.

9.18 No Liability Arising Solely From Lawful Termination. Except for obligations expressly stated in this Agreement and liabilities that cannot lawfully be waived, neither party shall be liable to the other solely because it properly exercised a contractual right to terminate or elected not to renew this Agreement. Any claim arising from termination remains subject to the exclusions and limitations stated in Section 6.3.

9.19 Survival. Termination or expiration shall not affect rights or obligations that accrued before the effective termination date. Provisions concerning payment, confidentiality, intellectual property, indemnification, limitations of liability, data handling, dispute resolution, and any other provisions that by their nature should survive shall remain effective after termination.

10. INSURANCE

10.1 General Insurance Requirement. During the term of this Agreement, each party shall maintain, at its own expense, insurance appropriate to its business operations, responsibilities, and risks under this Agreement and each Statement of Work. The insurance required by this Section shall be placed with insurers authorized to transact insurance in California or eligible to provide coverage through California's surplus-lines market.

10.2 Company Insurance. Company shall maintain the following insurance coverage:

10.2.1 Commercial General Liability. Commercial general liability insurance with limits of not less than $1,000,000 per occurrence and $2,000,000 in the aggregate, covering bodily injury, property damage, personal injury, advertising injury, products-completed operations, and contractual liability to the extent commercially available.

10.2.2 Workers' Compensation and Employers' Liability. Workers' compensation insurance in the amounts required by applicable law and employers' liability insurance with limits of not less than $1,000,000 per accident, $1,000,000 per employee for disease, and $1,000,000 in the aggregate for disease.

10.2.3 Commercial Automobile Liability. If Company-owned, hired, or non-owned motor vehicles are used in performing the Services, commercial automobile liability insurance with a combined single limit of not less than $1,000,000 per accident.

10.2.4 Technology Errors and Omissions and Cyber Liability. Technology errors and omissions and cyber-liability insurance, which may be maintained under separate policies or combined coverage, with limits of not less than $1,000,000 per claim and in the aggregate. Coverage shall address, as applicable, technology services, professional errors and omissions, network-security liability, privacy liability, unauthorized access, malware transmission, data incidents, and incident-response expenses.

10.3 Client Insurance. Client shall maintain the following insurance coverage, as applicable to its operations and the Services:

10.3.1 Commercial General Liability. Commercial general liability insurance with limits of not less than $1,000,000 per occurrence and $2,000,000 in the aggregate.

10.3.2 Workers' Compensation and Employers' Liability. Workers' compensation insurance in the amounts required by applicable law and employers' liability insurance with commercially reasonable limits.

10.3.3 Property Insurance. Commercial property insurance covering Client's premises, equipment, and other property against customary risks, including fire, theft, vandalism, water damage, and other causes of physical loss. Such insurance shall also cover Company-Owned Equipment located at Client's premises or under Client's possession or control for an amount not less than its full replacement cost.

10.3.4 Cyber and Privacy Insurance. Client shall maintain cyber and privacy liability insurance appropriate to the nature and volume of the data Client collects, stores, processes, or transmits and the risks associated with Client's operations. Unless otherwise stated in an Order or Statement of Work, such coverage shall have limits of not less than $1,000,000 per claim and in the aggregate.

10.4 Company-Owned Equipment. Company shall identify the Company-Owned Equipment furnished to Client and its applicable replacement value in an equipment schedule, Order, invoice, Statement of Work, or other written record. Client shall be responsible for physical loss of or damage to Company-Owned Equipment while located at Client's premises or under Client's possession or control, except to the extent caused by Company's negligence or willful misconduct. Client's responsibility shall not exceed the reasonable cost to repair or replace the affected equipment, less ordinary wear and tear.

10.5 Loss-Payee Status. Client shall cause Company to be identified as a loss payee under Client's applicable property insurance, but only with respect to Company-Owned Equipment and Company's insurable interest in that equipment. Insurance proceeds attributable to Company-Owned Equipment shall be payable to Company to the extent of Company's ownership interest and the covered loss.

10.6 Additional-Insured Status. To the extent commercially available under the applicable commercial general liability policy, each party shall name the other party and its officers, directors, members, managers, and employees as additional insureds, but only with respect to claims arising from the named insured's operations, acts, or omissions in connection with this Agreement. Additional-insured status does not apply to workers' compensation, technology errors-and-omissions, cyber-liability, or professional-liability coverage unless expressly endorsed by the applicable insurer.

10.7 Evidence of Insurance. Upon reasonable written request, each party shall provide the other with a certificate of insurance or other reasonable evidence demonstrating compliance with this Section. A certificate of insurance is provided for informational purposes only and does not amend, extend, or alter the coverage afforded by the underlying policy. Receipt or review of insurance evidence does not constitute approval of the coverage or waive any obligation under this Agreement.

10.8 Cancellation or Material Reduction. Each party shall use commercially reasonable efforts to provide prompt written notice after learning that a required policy has been canceled, nonrenewed, or materially reduced. Any insurer-provided notice shall be governed by the terms of the applicable policy and endorsement.

10.9 Deductibles and Self-Insured Retentions. Each party is responsible for its own deductibles, self-insured retentions, premiums, exclusions, and uninsured losses. Neither party shall take any action that knowingly invalidates or materially impairs insurance required under this Agreement.

10.10 Claims-Made Coverage. If any required technology errors-and-omissions, cyber-liability, or other professional-liability policy is written on a claims-made basis, the insured party shall maintain continuous coverage, an extended reporting period, or comparable replacement coverage for at least two years following termination of the applicable Services.

10.11 No Limitation of Liability. The insurance requirements in this Section do not expand or reduce either party's liability, indemnification obligations, or contractual limitations of liability. Failure to maintain required insurance does not relieve a party of any obligation or liability under this Agreement.

11. ACCEPTABLE USE; PROHIBITED AND UNLAWFUL ACTIVITIES

11.1 Lawful Use Requirement. Client shall use all equipment, software, networks, accounts, cloud services, communication services, security tools, and other technology furnished, hosted, supported, or managed by Company, collectively, the "Covered Technology," only for lawful business purposes and in compliance with this Agreement, applicable law, and applicable third-party provider terms.

11.2 Responsibility for Users. Client is responsible for the acts and omissions of its employees, contractors, agents, guests, and other persons who access or use Covered Technology through Client's accounts, credentials, devices, networks, or authority, collectively, "Authorized Users." Client shall maintain and enforce reasonable acceptable-use, access-control, and security policies governing its Authorized Users.

11.3 Prohibited Activities. Client shall not, and shall not permit any Authorized User or third party to, use Covered Technology to:

11.3.1 Violate any applicable federal, state, local, or foreign law, regulation, court order, or legally binding governmental requirement;

11.3.2 Infringe, misappropriate, or otherwise violate any copyright, patent, trademark, trade secret, privacy right, publicity right, contractual right, or other right belonging to another person;

11.3.3 Access or attempt to access any system, network, device, account, credential, data, or service without authorization or beyond the scope of authorized access;

11.3.4 Introduce, create, transmit, distribute, or facilitate malware, ransomware, viruses, worms, malicious code, credential-harvesting tools, denial-of-service activity, or other harmful or disruptive technology;

11.3.5 Interfere with, disrupt, damage, disable, overload, scan, probe, test, or circumvent the security or operation of any system, network, account, or service without express authorization;

11.3.6 Engage in fraud, identity theft, impersonation, phishing, payment diversion, financial deception, trafficking in stolen credentials, or any other deceptive or unlawful activity;

11.3.7 Sell, advertise, distribute, transmit, or facilitate products, services, content, or transactions that are illegal in the jurisdiction from which or to which they are offered, sold, shipped, transmitted, or delivered;

11.3.8 Publish, transmit, distribute, promote, or store unlawful obscene material, child sexual-abuse material, sexually exploitative content, credible threats of violence, unlawful harassment, or content that unlawfully discriminates against or targets a protected person or class;

11.3.9 Violate applicable export-control, economic-sanctions, privacy, data-protection, consumer-protection, anti-discrimination, communications, or intellectual-property laws; or

11.3.10 Assist, instruct, encourage, conceal, or facilitate any activity prohibited by this Section.

11.4 Electronic Communications and Commercial Email. Client shall not use Covered Technology to send or facilitate spam, abusive messaging, unauthorized bulk communications, or commercial electronic messages that violate applicable law or a provider's acceptable-use policy. Client is responsible for ensuring that its commercial email practices, including sender identification, subject lines, physical-address disclosures, opt-out mechanisms, suppression lists, and requests to stop receiving messages, comply with applicable law. This Section does not characterize every unsolicited commercial email as unlawful; it prohibits communications that violate applicable law, this Agreement, or applicable provider requirements.

11.5 Software Licensing. Client represents and warrants that all software installed, stored, accessed, or used on Covered Technology by or on behalf of Client is properly acquired, licensed, and used according to the applicable license terms. Upon reasonable request, Client shall provide evidence of licensing sufficient to allow Company to verify compliance. Company may decline to install, support, copy, migrate, or maintain software when Company reasonably believes the software is unauthorized, counterfeit, improperly licensed, or unlawfully obtained.

11.6 No Duty to Monitor. Unless expressly stated in the applicable Service Plan or Statement of Work, Company has no obligation to monitor Client's communications, content, or activities for legal compliance. Company's failure to detect, block, or report prohibited activity does not constitute approval of that activity or relieve Client of its obligations.

11.7 Investigation and Cooperation. If Company reasonably and in good faith suspects a violation of this Section, Client shall cooperate with Company's investigation and promptly provide relevant information within Client's possession or control. Company may preserve relevant logs, records, or data and may disclose information when authorized by Client or required by applicable law, a court order, subpoena, or other valid legal process.

11.8 Suspension and Termination. If Company reasonably and in good faith determines that Client's use of Covered Technology violates this Section or creates a material security, legal, operational, or reputational risk, Company may take proportionate protective action, including blocking affected traffic, disabling an account, isolating a device, suspending an affected Service, preserving evidence, or removing Company-Owned Equipment. Company may immediately suspend or terminate affected Services as provided in Section 9.5 when continued service would facilitate unlawful conduct, expose another person or system to harm, violate applicable law or provider requirements, or create a material risk that cannot reasonably be addressed through less restrictive measures. When practicable and legally permitted, Company shall notify Client of the action taken and provide a reasonable opportunity to correct the violation.

12. SERVICE AVAILABILITY; MAINTENANCE; REPORTING; REMEDIES

12.1 Scope of Availability Commitment. Company shall use commercially reasonable efforts to maintain the availability of any service that is hosted, operated, and directly controlled by Company, each a "Company-Controlled Service." No specific uptime percentage or availability guarantee applies unless expressly stated in the applicable Service Plan, Order, or Statement of Work, collectively, the "Availability Commitment." Monitoring, managing, supporting, or administering Client-owned or third-party technology does not make that technology a Company-Controlled Service.

12.2 Measurement of Availability. When an Availability Commitment applies, availability shall be measured during each calendar month using Company's monitoring records for the applicable Company-Controlled Service. Availability shall be calculated by subtracting qualifying Unscheduled Downtime from the total number of minutes in the applicable measurement period, excluding Scheduled Downtime and Excluded Downtime, and dividing the result by the total number of included minutes in that measurement period. Brief or intermittent events that do not materially prevent Client from using the applicable service shall not constitute Unscheduled Downtime.

12.3 Scheduled Maintenance. "Scheduled Downtime" means periods during which Company performs planned maintenance, upgrades, testing, repairs, replacements, security improvements, or other work affecting a Company-Controlled Service. When commercially practicable, Company shall schedule maintenance outside the hours of 8:00 a.m. through 5:00 p.m., Monday through Friday, and provide Client with at least forty-eight hours' advance notice. Company may perform maintenance during normal business hours with Client's authorization or when reasonably necessary to protect security, prevent service failure, address an urgent condition, comply with law, or avoid greater disruption. Emergency maintenance does not require advance notice, but Company shall notify Client as soon as reasonably practicable.

12.4 Excluded Downtime. "Excluded Downtime" means any unavailability, delay, degradation, interruption, or failure arising from or relating to one or more of the following circumstances:

12.4.1 Client Acts or Omissions. Any act, omission, error, delay, failure, misuse, or unauthorized activity by Client, an Authorized User, or a third party acting on Client's behalf.

12.4.2 Client Cooperation and Infrastructure. Client's failure to provide timely access, accurate information, required approvals, reasonable cooperation, supported equipment, adequate electrical power, environmental controls, or necessary connectivity.

12.4.3 Licensing and Payment Failures. Client's failure to pay a third-party provider, maintain or renew a required license, subscription, warranty, or support agreement, or comply with applicable third-party terms.

12.4.4 Third-Party Service Providers. The failure, suspension, degradation, maintenance, or unavailability of an internet service provider, telecommunications carrier, utility, cloud provider, data center, domain registrar, certificate authority, software publisher, hardware manufacturer, or other third-party provider.

12.4.5 Third-Party Platforms and Applications. The failure, suspension, degradation, maintenance, or unavailability of Microsoft 365, Microsoft Azure, Google Workspace, Google Cloud, Amazon Web Services, Slack, a customer-relationship management platform, accounting or payroll application, construction-management software, database system, or other third-party platform or application.

12.4.6 Client-Owned or Third-Party Technology. Any failure, incompatibility, defect, or degradation involving Client-owned or third-party hardware, software, networks, circuits, applications, accounts, configurations, integrations, or data.

12.4.7 Unsupported or Improperly Maintained Technology. Any failure involving technology that is unsupported, obsolete, unlicensed, modified without Company's authorization, improperly configured, or inadequately maintained.

12.4.8 Cybersecurity Events. A distributed denial-of-service attack, malware event, ransomware event, unauthorized access, security breach, malicious activity, or other cybersecurity event, except to the extent directly caused by Company's material breach of an express obligation under this Agreement.

12.4.9 Authorized Suspension or Termination. Any suspension, restriction, disconnection, or termination of Services authorized under this Agreement.

12.4.10 Client-Requested Activities. Any maintenance, testing, change, installation, configuration, upgrade, migration, or service interruption requested or authorized by Client.

12.4.11 Nonproduction Services. Any beta, trial, evaluation, preview, demonstration, testing, or no-charge service.

12.4.12 Force Majeure Events. Any Force Majeure Event as defined in this Agreement.

Downtime attributable to any circumstance identified in Sections 12.4.1 through 12.4.12 shall not count against an Availability Commitment or entitle Client to a service credit, refund, termination right, or other remedy under this Section.

12.5 Client-Caused Delays. If Company's performance is delayed, interrupted, or made more difficult by Client, an Authorized User, Client's environment, or a third-party dependency, Company shall receive a reasonable extension of the affected response time, milestone, delivery date, or performance period. Company may charge Client for additional work caused by the condition when that work is outside the applicable Service Plan.

12.6 Response and Resolution Times. A response-time commitment means the time within which Company will acknowledge an incident or begin initial triage during the applicable service period. A response-time commitment is not a guaranteed resolution time. Resolution depends on the nature of the issue, Client's cooperation, availability of parts and personnel, third-party provider performance, and other circumstances that may be outside Company's reasonable control.

12.7 Service Reports. Upon Client's reasonable written request, Company shall make available its standard service-availability report for the preceding calendar month when Company maintains reporting data for the applicable service. If an Availability Commitment was not met, the report shall identify the applicable measurement period, recorded Unscheduled Downtime, and the cause of the outage to the extent reasonably known. Company's monitoring records shall control unless Client provides reliable evidence demonstrating a material error.

12.8 Service-Credit Requests. If Company fails to satisfy an express Availability Commitment, Client may request a service credit by providing written notice within thirty days after the earlier of: (a) Company's delivery of the applicable monthly report; or (b) Client's discovery of the qualifying outage. The request must identify the affected service, date, approximate beginning and ending times, and reasonable supporting information. Client's failure to submit a timely and complete request waives the applicable service credit.

12.9 Calculation of Service Credit. Unless a different credit schedule is stated in the applicable Service Plan or Statement of Work, an approved service credit shall equal the monthly recurring fee paid for the affected Company-Controlled Service multiplied by the proportion of the applicable monthly measurement period during which the service experienced qualifying Unscheduled Downtime. A service credit shall not exceed the monthly recurring fee paid for the affected Company-Controlled Service for the month in which the outage occurred. Credits shall be applied to a future invoice and shall not be paid in cash. Fees for users, devices, hardware, software, licenses, third-party services, projects, consulting, and unaffected Services shall not be included in the calculation.

12.10 Exclusive Remedy. Except for Client's termination right under Section 12.11 and any liability that cannot lawfully be limited, an approved service credit shall be Client's sole and exclusive remedy for Company's failure to meet an Availability Commitment or other service level.

12.11 Persistent Availability Failure. If Company fails to satisfy the same express Availability Commitment for the same Company-Controlled Service during three consecutive calendar months, Client may provide Company with written notice describing the repeated failure. Company shall have thirty days after receiving notice to cure the condition or implement a commercially reasonable corrective plan. If Company fails to do so, Client may terminate the affected Company-Controlled Service without an early-termination charge by providing written notice within fifteen days after expiration of the cure period. Termination under this Section applies only to the affected service and does not terminate unrelated Services or this Agreement unless the failure materially defeats the principal purpose of the Agreement.

12.12 Initial Service Period. Availability Commitments do not apply during the first thirty days after Company begins onboarding Client or first implements the applicable service, collectively, the "Initial Service Period." The Initial Service Period allows Company to discover, document, configure, stabilize, patch, secure, and remediate Client's environment. This exception does not excuse Company from performing authorized Services in a professional and workmanlike manner.

12.13 No Warranty of Third-Party Availability. Company does not warrant or guarantee the availability, performance, security, compatibility, or continued operation of any Client-owned or third-party technology. Any credit or remedy offered by a third-party provider shall be governed by that provider's terms. Company may reasonably assist Client in pursuing an available third-party credit, but Company does not guarantee that the provider will approve or pay it.

13. CONFIDENTIALITY

13.1 Definitions. For purposes of this Section, the party disclosing Confidential Information is the "Disclosing Party," and the party receiving Confidential Information is the "Receiving Party." "Confidential Information" means any nonpublic information disclosed or made available by or on behalf of the Disclosing Party to the Receiving Party, whether orally, visually, electronically, in writing, through system access, or in any other form, that is marked or identified as confidential or that a reasonable person would understand to be confidential based on the nature of the information and the circumstances of disclosure.

13.2 Client Confidential Information. Client's Confidential Information includes Client Data, customer and employee information, customer lists, financial information, business records, contracts, internal communications, project information, plans, specifications, credentials, configurations, security information, personal information, and other nonpublic information concerning Client's business, personnel, customers, systems, or operations.

13.3 Company Confidential Information. Company's Confidential Information includes Company IP, pricing, quotes, proposals, discounts, service descriptions, solution designs, network designs, technical recommendations, security methods, internal documentation, credentials, configurations, scripts, automations, tools, templates, processes, procedures, vendor terms, cost information, personnel information, business plans, and other nonpublic information concerning Company's business, systems, services, or operations.

13.4 Exclusions. Confidential Information does not include information that the Receiving Party can demonstrate through competent evidence:

13.4.1 Public Information. Is or becomes publicly available through no breach of this Agreement or other wrongful act by the Receiving Party or a person acting on its behalf;

13.4.2 Previously Known Information. Was lawfully known to the Receiving Party without a confidentiality obligation before the Disclosing Party disclosed it;

13.4.3 Independently Developed Information. Was independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information; or

13.4.4 Third-Party Disclosure. Was lawfully received from a third party that, to the Receiving Party's knowledge, was not prohibited from disclosing it.

Information shall not fall within an exclusion merely because individual elements are publicly available if the particular compilation, arrangement, context, or application remains nonpublic.

13.5 Restrictions on Use and Disclosure. The Receiving Party shall:

13.5.1 Limited Use. Use the Disclosing Party's Confidential Information only as necessary to perform or receive the Services, exercise rights, enforce obligations, or otherwise fulfill the purposes of this Agreement;

13.5.2 Restricted Disclosure. Not disclose Confidential Information to any person except as expressly permitted by this Agreement or authorized in writing by the Disclosing Party;

13.5.3 Need-to-Know Access. Limit access to its employees, officers, professional advisors, insurers, financing sources, subcontractors, vendors, and service providers who have a legitimate need to know the information for purposes related to this Agreement; and

13.5.4 Confidentiality Obligations. Ensure that each person receiving Confidential Information is subject to confidentiality obligations or professional duties at least as protective as those applicable under this Section. The Receiving Party remains responsible for any unauthorized use or disclosure by a person to whom it provides access, except to the extent prohibited by applicable law.

13.6 Authorized Operational Use. Client authorizes Company and its approved employees, subcontractors, vendors, security providers, cloud providers, and professional advisors to access, process, transmit, store, and disclose Client Confidential Information to the extent reasonably necessary to provide, administer, secure, support, bill for, and improve the Services, respond to security events, comply with law, and enforce this Agreement. Company shall not sell Client Confidential Information or use it for an unrelated commercial purpose.

13.7 Standard of Care. Each Receiving Party shall protect the Disclosing Party's Confidential Information using at least the same degree of care it uses to protect its own confidential information of similar sensitivity, but in no event less than commercially reasonable care. Each party shall maintain reasonable administrative, technical, and physical safeguards appropriate to the nature and sensitivity of the Confidential Information within its possession or control.

13.8 Unauthorized Use or Disclosure. The Receiving Party shall notify the Disclosing Party without unreasonable delay after confirming any material unauthorized access, use, or disclosure of the Disclosing Party's Confidential Information. The Receiving Party shall take commercially reasonable steps to contain and mitigate the unauthorized activity and shall reasonably cooperate with the Disclosing Party's response. This provision does not replace any more specific security-incident or data-breach obligations stated elsewhere in this Agreement or required by applicable law.

13.9 Compelled Disclosure. If the Receiving Party is required by applicable law, subpoena, court order, civil investigative demand, regulatory request, or other valid legal process to disclose Confidential Information, the Receiving Party may make the required disclosure, provided that, to the extent legally permitted and reasonably practicable, it:

13.9.1 Notice. Promptly provides the Disclosing Party with written notice sufficient to permit the Disclosing Party to seek a protective order or other appropriate remedy;

13.9.2 Cooperation. Provides reasonable assistance requested by the Disclosing Party in seeking protection, at the Disclosing Party's expense; and

13.9.3 Limited Disclosure. Discloses only the portion of the Confidential Information that the Receiving Party is legally required to disclose and uses reasonable efforts to obtain confidential treatment for the disclosed information.

If notice is prohibited by law or legal process, the Receiving Party may disclose the required information without providing notice and without breaching this Agreement.

13.10 Return or Destruction. Upon the Disclosing Party's written request or termination of this Agreement, the Receiving Party shall, subject to the transition, data-retention, and intellectual-property provisions of this Agreement, return or securely destroy the Disclosing Party's Confidential Information within its possession or control. The Receiving Party may retain copies:

13.10.1 Legal Retention. To the extent required by applicable law, regulation, court order, professional obligation, insurance requirement, or bona fide record-retention policy; and

13.10.2 Backup Systems. Within routine backup, archival, disaster-recovery, security, or logging systems when deletion is not reasonably practicable.

Any retained Confidential Information shall remain protected by this Agreement and shall not be accessed or used except for the purpose requiring its retention or through ordinary backup-restoration procedures.

13.11 No Transfer of Ownership. Disclosure of Confidential Information does not transfer ownership, grant a license, or convey any intellectual-property right except for the limited rights expressly granted under this Agreement.

13.12 Equitable Relief. Each party acknowledges that unauthorized use or disclosure of Confidential Information may cause harm that cannot be adequately remedied by monetary damages alone. The Disclosing Party may seek temporary, preliminary, or permanent injunctive relief and other equitable remedies for an actual or threatened breach of this Section, without limiting any other remedy available under this Agreement or applicable law.

13.13 Duration and Survival. The obligations in this Section shall continue during the term of this Agreement and for five years after its termination or expiration. Confidential Information qualifying as a trade secret shall remain protected for as long as it continues to qualify as a trade secret under applicable law. Obligations concerning personal information, protected data, and legally regulated information shall survive for the period required by applicable law.

14. GENERAL CONTRACT PROVISIONS

14.1 Assignment. Neither party may assign, delegate, or otherwise transfer this Agreement, any Statement of Work, or any material right or obligation arising under them without the other party's prior written consent, which shall not be unreasonably withheld, conditioned, or delayed. Any attempted assignment that does not comply with this Section is void.

14.1.1 Permitted Corporate Assignment. Either party may assign this Agreement and any affected Statement of Work without the other party's consent in connection with a merger, consolidation, reorganization, change of control, or sale of all or substantially all of the assigning party's business or assets to which this Agreement relates, provided that all of the following conditions are satisfied:

14.1.1.1 Written Assumption of Obligations. The assignee agrees in writing to assume and perform all applicable obligations of the assigning party under this Agreement and each affected Statement of Work.

14.1.1.2 Preservation of Contractual Rights. The assignment does not materially reduce, impair, or adversely affect the nonassigning party's rights, remedies, protections, or expected benefits under this Agreement.

14.1.1.3 Ability to Perform. The assignee possesses the financial resources, operational capabilities, personnel, licensing, and legal authority reasonably necessary to perform the assigned obligations.

14.1.1.4 Notice of Assignment. The assigning party provides the nonassigning party with prompt written notice identifying the assignment, its effective date, and the identity and contact information of the assignee.

14.1.2 Assignment to a Competitor. Client may not assign this Agreement or disclose Company's Confidential Information to a direct competitor of Company without Company's prior written consent.

14.1.3 Subcontracting Distinguished. Company's engagement of employees, subcontractors, vendors, cloud providers, or other service providers to assist in performing the Services does not constitute an assignment and is governed by the subcontracting provisions of this Agreement.

14.1.4 Binding Effect. Subject to the restrictions in this Section, this Agreement and each Statement of Work shall bind and benefit the parties and their respective permitted successors and assigns.

14.2 Entire Agreement. This Agreement, together with its schedules, exhibits, Orders, Service Plans, and Statements of Work expressly incorporated into it, constitutes the entire agreement between the parties concerning its subject matter and supersedes all prior or contemporaneous proposals, negotiations, communications, representations, promises, understandings, and agreements concerning that subject matter, whether oral or written.

Neither party has relied upon any representation, promise, warranty, or statement that is not expressly stated in an executed contract document. Marketing materials, website content, brochures, presentations, demonstrations, estimates, and other descriptive materials are provided for general informational purposes and do not modify this Agreement or create a binding obligation unless expressly incorporated into an Order or Statement of Work.

14.3 Amendments and Modifications. No amendment, modification, waiver, or supplement to this Agreement, any Service Plan, or any Statement of Work shall be effective unless it is in writing, expressly identifies the contract document being modified, and is signed by an authorized representative of each party. An email, service ticket, meeting note, or oral instruction does not amend this Agreement unless it clearly states the parties' intent to amend the Agreement and is approved by authorized representatives of both parties.

14.4 Order of Precedence. In the event of a direct conflict among the documents governing the Services, the order-of-precedence provisions stated in Section 1 shall apply. A document shall modify another contract document only to the extent it expressly identifies the provision being modified and states the parties' intent to override that provision.

14.5 No Waiver. A party's failure or delay in exercising or enforcing any right, remedy, term, or condition shall not constitute a waiver. A waiver is effective only if it is in writing and signed by the party granting it, and any waiver shall apply only to the specific circumstance for which it was granted. A party's waiver of one breach does not waive any previous, continuing, or subsequent breach. The granting of additional time for performance does not waive the requirement of future timely performance.

14.6 Force Majeure. Neither party shall be liable for a delay or failure to perform an obligation under this Agreement or a Statement of Work to the extent caused by an event beyond that party's reasonable control and not resulting from its negligence or willful misconduct, a "Force Majeure Event."

14.6.1 Covered Events. Force Majeure Events may include natural disasters, earthquakes, fires, floods, severe weather, epidemics, pandemics, war, terrorism, civil unrest, sabotage, labor disputes, governmental actions, embargoes, supply-chain disruptions, transportation delays, utility failures, internet or telecommunications outages, widespread cloud-service interruptions, cyberattacks, and shortages of equipment, materials, or qualified personnel.

14.6.2 Notice and Mitigation. The affected party shall notify the other party as soon as reasonably practicable and shall use commercially reasonable efforts to mitigate the effects of the Force Majeure Event and resume performance.

14.6.3 Extension of Performance. The time for the affected performance shall be extended for a reasonable period corresponding to the duration and effect of the Force Majeure Event.

14.6.4 Payment Obligations. A Force Majeure Event does not excuse Client from paying amounts that accrued before the event or amounts due for Services, licenses, subscriptions, products, or third-party commitments that continue during the event.

14.6.5 Extended Force Majeure Event. If a Force Majeure Event materially prevents performance of a substantial portion of the Services for more than sixty consecutive days, either party may terminate the materially affected Services by written notice without an early-termination charge. Client remains responsible for accrued amounts and authorized noncancelable commitments.

14.7 Contractual Limitation Period. To the maximum extent permitted by applicable law, any lawsuit, arbitration, or other proceeding arising out of or relating to this Agreement, a Statement of Work, or the Services must be commenced within one year after the claim accrues. A claim not commenced within that period is permanently barred.

The one-year limitation does not apply to: (a) an action by Company to collect unpaid fees or other amounts due; (b) a claim for indemnification that has not accrued because the applicable third-party claim has not been asserted or resolved; (c) unauthorized use or infringement of intellectual-property rights; (d) misappropriation of trade secrets; (e) breach of confidentiality; or (f) any claim for which applicable law prohibits contractual shortening of the limitations period.

14.8 Severability and Reformation. If a court or other tribunal of competent jurisdiction determines that any provision of this Agreement or a Statement of Work is invalid, illegal, or unenforceable, that provision shall be enforced to the maximum extent permitted by law. If necessary, the provision shall be modified only to the minimum extent required to make it valid and enforceable while preserving the parties' original intent as closely as possible. The remaining provisions shall remain in full force and effect.

14.9 Purchase Orders and Administrative Documents. Any purchase order, vendor-registration form, procurement document, portal entry, confirmation, memorandum, email, invoice instruction, or other administrative document issued or required by Client is for Client's internal administrative convenience only. Any additional or conflicting term contained in such a document is rejected and shall not modify this Agreement, even if Company acknowledges, signs, processes, accepts payment under, or performs Services in response to that document. Such terms shall become binding only through a written amendment satisfying Section 14.3.

14.10 Authority. Each person signing this Agreement, an Order, or a Statement of Work represents that the person is authorized to bind the party on whose behalf the person signs. Each party represents that its execution and performance of the applicable agreement do not violate any other agreement or legal obligation binding upon that party.

14.11 Further Assurances. Each party shall execute and deliver any additional documents and take any reasonable actions necessary to carry out the express purposes of this Agreement, provided those documents or actions do not materially expand that party's obligations without its written consent.

15. GOVERNING LAW; EXCLUSIVE JURISDICTION AND VENUE

15.1 Governing Law. This Agreement, each Service Plan, Order, and Statement of Work, and any dispute, claim, or controversy arising out of or relating to them or the Services shall be governed by and construed under the laws of the State of California, without regard to California's conflict-of-laws principles that would require application of another jurisdiction's laws.

15.2 Exclusive Jurisdiction and Venue. Subject to any dispute-resolution procedure expressly stated elsewhere in this Agreement, each party shall bring any lawsuit or judicial proceeding arising out of or relating to this Agreement, a Service Plan, an Order, a Statement of Work, or the Services exclusively in:

15.2.1 State-Court Proceedings. The Superior Court of California for the County of San Bernardino; or

15.2.2 Federal-Court Proceedings. If federal subject-matter jurisdiction exists, the United States District Court for the Central District of California, Eastern Division.

15.3 Consent to Jurisdiction. Each party irrevocably submits to the personal jurisdiction of the courts identified in Section 15.2 and waives, to the fullest extent permitted by law, any objection based on lack of personal jurisdiction, improper venue, inconvenient forum, or any similar ground.

15.4 Federal Jurisdiction Unavailable. If a federal court lacks subject-matter jurisdiction or declines to exercise jurisdiction, the applicable action shall be brought exclusively in the Superior Court of California for the County of San Bernardino.

15.5 Equitable Relief in Another Jurisdiction. Notwithstanding Section 15.2, a party may seek temporary, preliminary, or emergency equitable relief in another court of competent jurisdiction when reasonably necessary to protect Confidential Information, intellectual-property rights, Company-Owned Equipment, data, systems, or other property from immediate or irreparable harm. Seeking such relief does not waive the exclusive forum for deciding the underlying dispute.

15.6 United Nations Convention Excluded. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement or any transaction governed by it.

16. ADDITIONAL AND MISCELLANEOUS TERMS

16.1 Protection Against Improper Interference. During the term of this Agreement and for one year after its termination, Client shall not knowingly use Company's Confidential Information, trade secrets, or other unlawful means to induce a Company employee, independent contractor, or subcontractor to breach an existing contractual obligation owed to Company or to improperly divert Company personnel, customers, business opportunities, or proprietary information.

16.1.1 Permitted Employment Activity. Nothing in this Agreement prohibits any person from engaging in a lawful profession, trade, or business. This Section does not prohibit Client from:

16.1.1.1 General Solicitation. Publishing a general employment advertisement, conducting a general recruiting campaign, or using a recruiting firm that does not specifically target Company personnel;

16.1.1.2 Unsolicited Contact. Communicating with or hiring a Company employee, independent contractor, or subcontractor who independently contacts Client without direct or indirect solicitation by Client;

16.1.1.3 Prior Relationship. Communicating with a person with whom Client had a documented business or employment relationship before Company assigned that person to perform Services for Client; or

16.1.1.4 Lawful Hiring. Otherwise engaging in hiring or recruitment activity protected by applicable law.

16.1.2 Available Remedies. A violation of Section 16.1 constitutes a material breach of this Agreement. Company may pursue damages and equitable relief available under applicable law, subject to the limitations and procedures stated in this Agreement. This Section does not impose a predetermined hiring fee, liquidated-damages payment, or restriction on lawful employee mobility.

16.2 No Third-Party Beneficiaries. Except for an Indemnified Party expressly protected under Section 7 or another person expressly identified in this Agreement as having an enforceable right, this Agreement is entered into solely for the benefit of Company and Client. No other person or entity may rely upon, enforce, or claim any right or remedy under this Agreement.

16.3 No Modification by Trade Usage or Course of Dealing. No usage of trade, course of dealing, course of performance, prior practice, or customary industry practice shall modify, supplement, explain, waive, or alter an express provision of this Agreement, a Service Plan, an Order, or a Statement of Work.

16.4 Business Day. "Business Day" means any day other than Saturday, Sunday, or a holiday observed by banks or state courts in California. If a deadline stated in this Agreement falls on a day that is not a Business Day, the deadline shall be extended through the end of the next Business Day. This provision does not extend a payment deadline, response period, or other obligation expressly measured in calendar days unless the applicable provision states otherwise.

16.5 Notices. Any formal notice required or permitted under this Agreement shall be in writing and delivered to the applicable party at the physical or email address identified in this Agreement, the applicable Order, or a later written notice updating that address.

16.5.1 Permitted Delivery Methods. Formal notices may be delivered by personal delivery, nationally recognized overnight courier, certified United States mail with return receipt requested, or email.

16.5.2 Effective Date of Notice. A notice shall be deemed received:

16.5.2.1 Personal Delivery. On the date it is personally delivered;

16.5.2.2 Overnight Courier. On the date shown in the courier's delivery confirmation;

16.5.2.3 Certified Mail. Three Business Days after deposit with the United States Postal Service, postage prepaid, unless delivery records establish an earlier or later date of actual receipt; or

16.5.2.4 Email. On the date transmitted if sent before 5:00 p.m. Pacific Time on a Business Day and the sender does not receive a delivery-failure or rejection notice. An email sent after 5:00 p.m. Pacific Time or on a non-Business Day shall be deemed received on the next Business Day.

16.5.3 Legal Notices to Company. A notice asserting breach, default, indemnification, termination, or a legal claim against Company must be sent both by email and by personal delivery, overnight courier, or certified mail. Operational communications, service tickets, support requests, project messages, and billing inquiries do not constitute formal legal notice unless they expressly state that they are intended as notice under this Agreement.

16.6 Independent Contractors. The parties are independent contractors. Nothing in this Agreement creates an employment, partnership, joint venture, fiduciary, franchise, agency, or similar relationship between the parties. Neither party has authority to bind the other, incur an obligation on the other's behalf, or make a representation or warranty for the other unless expressly authorized in writing. Each party is responsible for the compensation, supervision, direction, taxes, benefits, insurance, and conduct of its own personnel.

16.7 Subcontractors and Service Providers. Company may engage employees, independent contractors, subcontractors, vendors, cloud providers, security providers, and other third parties to perform or support any portion of the Services.

16.7.1 Company Responsibility. Company remains responsible for the performance of Company-designated subcontractors to the same extent Company would be responsible if Company performed the applicable Services directly, subject to the exclusions and limitations stated in this Agreement.

16.7.2 Third-Party Products and Services. Company does not guarantee the performance, availability, security, or quality of independent Third-Party Products or third-party services governed by their own provider terms merely because Company procures, configures, administers, or supports them.

16.7.3 Confidentiality and Security. Company shall require subcontractors that receive Confidential Information to maintain confidentiality and security obligations appropriate to the nature of the information and the services they perform.

16.7.4 Nondelegable Services. Company shall not delegate a Service expressly designated as nondelegable in a Statement of Work signed by Company. A unilateral designation by Client does not make a Service nondelegable.

16.7.5 No Employment Relationship. Company's subcontractors and personnel remain under Company's or the applicable subcontractor's direction and control and shall not be considered Client's employees, agents, or joint employees.

16.8 Counterparts and Electronic Signatures. This Agreement, any Order, amendment, and Statement of Work may be executed in any number of counterparts. Each executed counterpart shall be deemed an original, and all counterparts together shall constitute one instrument.

Signatures delivered electronically, including through an electronic-signature platform, a scanned or electronically reproduced handwritten signature, or another method demonstrating the signer's intent to sign, shall have the same force and effect as an original handwritten signature. Each party may rely upon the apparent authenticity and integrity of an electronic signature unless it has actual knowledge that the signature is unauthorized.

16.9 Confidentiality and Restricted Disclosure of Company Proposals. Company's quotes, proposals, Statements of Work, pricing schedules, discounts, service descriptions, assessments, technical recommendations, solution designs, diagrams, and related materials, collectively, "Company Proposal Materials," constitute Company Confidential Information under Section 13 and are intended solely for Client and Client's authorized representatives.

16.9.1 Prohibited Disclosure. Client shall not disclose, distribute, reproduce, publish, transmit, or otherwise make Company Proposal Materials available to any competitor, vendor, consultant, prospective service provider, or other third party without Company's prior written consent.

16.9.2 Permitted Professional Disclosures. Client may disclose Company Proposal Materials to its attorneys, accountants, insurers, financing sources, and other professional advisors who have a legitimate need to review them, provided that each recipient is informed of their confidential nature and is subject to confidentiality obligations or professional duties at least as protective as those stated in this Agreement.

16.9.3 Internal Access. Client may disclose Company Proposal Materials to its officers and employees who have a legitimate need to evaluate, approve, administer, or receive the proposed Services, subject to Client's responsibility for compliance with this Section.

16.9.4 Competitive Procurement. Client may use Company Proposal Materials internally to evaluate Company's offering but shall not disclose Company's nonpublic pricing, service design, scope, recommendations, or other proprietary content to another provider for purposes of obtaining a competing quote, duplicating Company's solution, or negotiating another provider's pricing.

16.9.5 Unauthorized Disclosure. Unauthorized disclosure or use of Company Proposal Materials constitutes a material breach of this Agreement. Company may seek injunctive relief, actual damages, and any other remedy available under this Agreement or applicable law. Any recovery of attorneys' fees or costs shall be governed by the applicable attorneys' fees provision, another express contractual right, or applicable law.

16.9.6 Survival. Client's obligations under this Section shall survive expiration, rejection, withdrawal, or termination of the applicable quote, proposal, Statement of Work, or Agreement for the period stated in Section 13.13. Information qualifying as a trade secret shall remain protected for as long as it retains that status under applicable law.

17. SYSTEM ACCESS; CREDENTIALS; CONTRACT UPDATES

17.1 Authorization to Access Covered Systems. Client authorizes Company and its approved personnel and subcontractors to access Client's covered systems, networks, devices, accounts, applications, cloud services, and other technology to the extent reasonably necessary to provide the Services. This authorization includes remote and onsite administrative access when included in the applicable Service Plan, Order, or Statement of Work.

17.2 Required Credentials and Permissions. Client shall provide or authorize Company to establish the administrative credentials, service accounts, application permissions, security roles, authentication methods, and other access reasonably necessary to perform the Services. Company shall not be required to perform work for which Client has not provided adequate authorization, credentials, permissions, or access.

17.3 Least-Privilege Access. When technically and operationally practicable, Company shall use role-based and least-privilege access appropriate to the Services being performed. Company may maintain administrative or emergency access when reasonably necessary to monitor, secure, support, recover, or administer the covered environment.

17.4 Service and Administrative Accounts. Client authorizes Company to create, configure, maintain, rotate, disable, and remove administrative, service, monitoring, backup, security, and integration accounts reasonably necessary to provide the Services. Such accounts shall be used only for authorized business purposes.

17.5 Credential Security. Company shall use commercially reasonable safeguards to protect Client credentials within Company's possession or control. Such safeguards may include multifactor authentication, privileged-access controls, encrypted credential storage, access logging, credential rotation, and restrictions based on personnel roles.

17.6 Client Credential Responsibilities. Client shall:

17.6.1 Accurate Access Information. Provide accurate and current credentials, account information, authorization, and access instructions;

17.6.2 Secure Transmission. Use Company's approved secure method when transmitting passwords, authentication codes, recovery keys, or other sensitive access information;

17.6.3 Authorized Access. Ensure that Client has the legal and contractual authority to grant Company access to the applicable systems, accounts, applications, and data;

17.6.4 Security Changes. Promptly notify Company of any suspected credential compromise, unauthorized access, personnel change, ownership dispute, or other circumstance affecting Company's authorized access; and

17.6.5 Access Continuity. Refrain from disabling, changing, or restricting Company-managed accounts or security tools without prior coordination when doing so could interfere with the Services or create a security risk.

17.7 Personal Credentials. Company may require a dedicated administrative or service account instead of using an employee's personal credentials. Client shall not require Company personnel to share individual Company credentials or disclose authentication methods that would violate Company's security policies.

17.8 Delayed or Restricted Access. Company shall not be responsible for a delay, service interruption, missed service level, or failure to perform caused by Client's failure to provide or maintain required access. Company shall receive a reasonable extension of any affected deadline and may charge for additional work resulting from delayed, incomplete, or improperly configured access.

17.9 Access Upon Termination. Upon expiration or termination of the applicable Services, Company may disable or remove Company-controlled accounts, tools, agents, credentials, and access methods as provided in

Sections 8 and 9. Company shall provide Client-owned credentials and other required transition information subject to Client's payment and transition obligations.

17.10 Reference Copy of Agreement. Company may maintain a reference copy of its then-current standard agreement terms at https://www.trinitynetworx.com/TN-terms/. The online copy is provided for reference and administrative convenience. If the online copy conflicts with an Agreement executed by the parties, the executed Agreement controls.

17.11 Amendments to Executed Agreement. Company may not materially amend an executed Agreement merely by posting revised terms online. Any amendment to an executed Agreement must comply with Section 14.3 unless the Agreement expressly identifies a particular online policy that may be updated under Section 17.12.

17.12 Operational Policies and Technical Standards. Company may periodically update its reasonable operational policies, security requirements, supported-technology standards, service procedures, and acceptable-use requirements to address changes in law, technology, cybersecurity risk, insurance requirements, or third-party provider obligations. Company shall provide reasonable notice of any material update. An operational update shall not materially reduce Client's purchased Services, materially increase Client's recurring fees, or alter the fundamental allocation of liability without Client's written agreement.

17.13 Renewal Terms. Company may propose updated agreement terms in connection with a renewal, replacement Order, or material change in Services. Updated terms become binding only when accepted by Client through a signed renewal, Order, amendment, or other legally sufficient written acceptance.

18. THIRD-PARTY PRODUCTS AND PROVIDERS

18.1 Use of Third-Party Providers. Company may procure, resell, configure, administer, support, integrate, or otherwise use third-party hardware, software, licenses, subscriptions, cloud services, telecommunications services, security services, backup platforms, data centers, and other products or services, collectively, "Third-Party Services," in connection with the Services.

18.2 Third-Party Terms. Client's access to or use of a Third-Party Service may be subject to the provider's license agreement, subscription terms, acceptable-use policy, privacy terms, data-processing terms, warranty, service-level agreement, or other contractual requirements, collectively, "Third-Party Terms." Client agrees to comply with Third-Party Terms applicable to Third-Party Services authorized, purchased, or used by Client.

18.3 Disclosure of Applicable Providers and Terms. Company may identify commonly used third-party providers and provide links to available Third-Party Terms at https://www.trinitynetworx.com/thirdparty-terms/, in an Order, in a Statement of Work, through a provider portal, or in other service documentation. The website list is provided for reference and may not identify every incidental subcontractor, infrastructure provider, or component used to deliver the Services.

18.4 Client Acceptance of Provider Terms. When a provider requires Client's direct acceptance of Third-Party Terms, account registration, identity verification, payment method, or electronic signature, Client shall timely complete the required process. Company is not responsible for a delay, suspension, or inability to provide an affected Service caused by Client's failure or refusal to accept applicable Third-Party Terms.

18.5 Limited Authority to Act for Client. Client authorizes Company to establish, configure, administer, and manage Third-Party Services on Client's behalf to the extent reasonably necessary to implement services that Client has approved. Company may accept routine provider terms on Client's behalf when acceptance is technically required to provision an authorized Third-Party Service. Company has no authority to accept a material financial commitment, unusual liability, or unrelated service on Client's behalf without Client's authorization.

18.6 Provider Changes to Terms. A third-party provider may modify its Third-Party Terms, pricing, features, licensing, support, security controls, data practices, or service availability. Such changes are controlled by the provider and may become effective according to the provider’s terms. Company shall use commercially reasonable efforts to notify Client of a material change known to Company that materially affects the Services, but Company is not responsible for a provider’s failure to give notice or for changes outside Company’s control.

18.7 Replacement or Discontinuation of Provider. Company may replace a third-party provider or Third-Party Service when reasonably necessary because of availability, security, compatibility, performance, pricing, licensing, legal compliance, vendor support, or business continuity. Company shall use commercially reasonable efforts to provide advance notice if the replacement materially affects Client’s Services, fees, data location, or operations.

If a Third-Party Service becomes unavailable or commercially unreasonable to continue, Company may discontinue the affected Service or propose a replacement. Any material change in recurring fees or scope shall require Client’s approval unless the applicable Order expressly permits pass-through price adjustments.

18.8 Third-Party Charges and Commitments. Client is responsible for approved third-party license fees, subscriptions, usage charges, taxes, price increases, minimum commitments, and early-termination charges. Unless expressly stated otherwise, third-party charges are nonrefundable after Company places the applicable order or the provider activates the service.

18.9 Third-Party Data Processing. Client authorizes Company to provide applicable third-party providers with access to Client Data to the extent reasonably necessary to deliver, secure, administer, or support an authorized Third-Party Service. Company shall require providers under its direct contractual control to maintain confidentiality and security obligations appropriate to the services they perform, subject to the provider’s standard terms and applicable law.

18.10 Third-Party Performance. Company does not control and is not responsible for a third-party provider’s acts, omissions, outages, security incidents, product defects, service changes, discontinuation, data loss, or failure to satisfy its contractual obligations. Company may reasonably assist Client in addressing a provider issue, but Company does not guarantee the outcome, performance, security, availability, or continued operation of any Third-Party Service.

18.11 Provider Warranties and Remedies. Third-Party Services are subject to the warranty, support, credit, refund, and remedy terms offered by the applicable provider. To the extent legally and contractually permitted, Company shall pass through to Client any applicable provider warranty or service credit actually received for Client’s affected service. Company is not required to provide a greater warranty, credit, refund, or remedy than Company receives from the provider.

18.12 Conflicting Terms. Third-Party Terms govern Client’s use of the applicable Third-Party Service and the relationship between Client and the provider. This Agreement governs the relationship between Client and Company. If Third-Party Terms prevent Company from performing an obligation under this Agreement, Company shall notify Client and the parties shall work in good faith to determine whether the affected Service can be modified, replaced, or discontinued.

18.13 Suspension and Termination. A third-party provider may suspend or terminate a Third-Party Service according to its Third-Party Terms. Company may suspend an affected Service if Client violates applicable Third-Party Terms or if continued use creates a material legal, security, financial, or operational risk. Termination of this Agreement does not eliminate Client’s responsibility for authorized noncancelable third-party commitments.

18.14 No Undisclosed Material Reduction. Company’s use or replacement of a third-party provider shall not permit Company to materially reduce the core scope of Client’s purchased Service Plan without Client’s written agreement. Changes that are reasonably equivalent in function, security, and service purpose do not constitute a material reduction.

EXHIBIT 1

TRINITY FOUNDATION

Co-Managed Information Technology Services

This Exhibit 1 is incorporated into the Master Services Agreement between Trinity Networx, LLC (“Company”) and the Client identified in the Agreement. This Exhibit defines the scope, allocation of responsibilities, limitations, and commercial controls applicable to the Trinity Foundation Service Plan. Capitalized terms not defined in this Exhibit have the meanings assigned in the Agreement.

1. SERVICE-PLAN PURPOSE

1.1 Co-Managed Service Model. Trinity Foundation is a co-managed information technology service plan intended for a Client that continuously maintains qualified internal information technology personnel capable of performing routine end-user support, daily administration, and first-level troubleshooting.

1.2 Shared Responsibility. Company supplements Client’s internal information technology resources. Company does not assume primary responsibility for all end-user support, cybersecurity, compliance, infrastructure, business continuity, or technology operations.

1.3 Required Internal Resource. Client shall designate at least one qualified internal information technology contact with sufficient authority, availability, technical ability, and access to coordinate with Company. If Client no longer maintains that resource, Company may require transition to Trinity Complete or another appropriate plan.

2. INCLUDED SERVICES

2.1 Remote Monitoring and Management. Company shall deploy and administer its approved remote monitoring and management tools on supported covered devices. Monitoring may include device availability, operating-system status, hardware conditions, selected services, and configured alert conditions.

2.2 Patch Management. Company shall manage generally available operating-system patches and approved third-party application updates for supported covered devices when technically and commercially practicable. Company may defer or exclude updates that present stability, compatibility, licensing, or operational concerns.

2.3 Endpoint Detection and Response. Company shall deploy and administer its approved endpoint detection and response platform on supported covered endpoints for which required licensing has been purchased or expressly included.

2.4 Infrastructure Monitoring. Company shall monitor supported covered servers, firewalls, switches, wireless equipment, and other infrastructure expressly identified in Company’s records. Monitoring does not include replacement hardware, manufacturer support, licensing, remediation, configuration changes, or onsite response unless expressly included.

2.5 Microsoft 365 Administration. Company shall provide escalation-level administration of Client’s supported Microsoft 365 tenant, including assistance with covered account, license, access, and configuration issues that Client’s internal information technology personnel cannot reasonably resolve.

2.6 Documentation and Asset Information. Company shall maintain internal technical documentation concerning the covered environment, including available configuration, asset, credential, and vendor information. Company’s internal operating procedures, tool configurations, templates, security methods, and proprietary documentation remain Company property.

2.7 Escalation Support. Company shall provide remote escalation assistance to Client’s designated information technology personnel for covered systems and services. Escalation support does not constitute unlimited direct support for Client’s employees.

2.8 Reporting and Review. Company shall provide periodic service reporting and a quarterly technology review, subject to Client's reasonable cooperation and attendance.

3. CLIENT RESPONSIBILITIES

3.1 First-Level Support. Client's internal information technology personnel shall serve as the first point of contact for Client's employees and shall perform routine troubleshooting, password assistance, user guidance, workstation preparation, peripheral support, and other ordinary end-user functions.

3.2 User Administration. Unless otherwise agreed in writing, Client shall handle routine onboarding, offboarding, account changes, permissions, group membership, equipment assignment, application access, and user training.

3.3 Escalation Information. Before escalating an issue, Client shall perform reasonable initial troubleshooting and provide relevant error messages, logs, screenshots, affected-user information, steps already taken, and other reasonably requested information.

3.4 Access and Cooperation. Client shall provide timely access to covered systems, facilities, vendors, personnel, credentials, records, and decision-makers reasonably necessary to provide the Services.

3.5 Supported Standards. Client shall maintain supported hardware, software, operating systems, licensing, warranties, connectivity, and vendor support. Company is not responsible for delays or failures caused by unsupported, unlicensed, obsolete, or improperly maintained technology.

4. SUPPORT COVERAGE

4.1 Business-Hours Escalation Coverage. Covered escalation support is provided during Normal Business Hours. Direct end-user support, onsite work, after-hours work, and emergency response are excluded unless expressly authorized and separately billed.

4.2 Monitoring Distinguished From Remediation. Twenty-four-hour monitoring refers to automated monitoring and alert generation. It does not mean continuous human staffing, investigation, remediation, or unlimited after-hours support.

4.3 Response Targets. Any response target applies only to properly submitted Trouble Tickets during the applicable service period and refers to acknowledgment or commencement of triage, not guaranteed resolution.

5. SERVICES NOT INCLUDED

5.1 Direct End-User Help Desk. Unlimited or routine direct end-user help desk services are not included.

5.2 Onboarding and Offboarding. Routine onboarding, offboarding, workstation deployment, equipment retrieval, and account administration are not included.

5.3 Onsite and After-Hours Services. Onsite services, field dispatch, jobsite visits, travel, mileage, after-hours services, weekend services, and holiday services are separately billable.

5.4 Projects and Remediation. Projects, migrations, installations, relocations, new-location deployments, major configuration changes, incident response, forensic analysis, compromise remediation, and correction of preexisting conditions or technical debt are excluded.

5.5 Products and Third-Party Charges. Hardware, software, licenses, subscriptions, cloud consumption, telecommunications, internet, backup, security, firewall, server, manufacturer-support, and other third-party charges are excluded unless expressly listed as included.

5.6 Specialized and Compliance Services. Penetration testing, vCISO services, policy drafting, compliance certification, formal audits, legal advice, and cyber-insurance certification are excluded unless separately authorized.

6. COVERED ENVIRONMENT

6.1 Covered Environment. Services apply only to users, devices, systems, accounts, locations, and other assets identified as covered in Company's records and for which applicable fees have been paid.

6.2 Unmanaged Technology. Company is not responsible for technology that is not enrolled in Company's approved tools or within Company's authorized management and control.

6.3 Environmental Changes. Client shall notify Company before adding users, devices, systems, applications, vendors, or locations that may affect scope, risk, licensing, or fees.

7. ADDITIONAL SERVICES AND CHARGES

7.1 Separate Authorization. Services outside this Exhibit require authorization and may be billed under a Statement of Work or at Company's applicable hourly rates.

7.2 Minimum Monthly Commitment. The minimum monthly recurring charge stated in the applicable Order applies regardless of actual user count, device count, or service usage.

7.3 Scope Reassessment. Company may recommend or require a service-plan change if Client's environment, staffing, risk, support demand, locations, or regulatory requirements materially change.

8. SERVICE LIMITATIONS

8.1 No Guaranteed Prevention. Monitoring, patching, and endpoint protection reduce risk but cannot guarantee detection or prevention of every threat, failure, vulnerability, or unauthorized activity.

8.2 Third-Party Dependencies. Company is not responsible for outages, defects, delays, or changes attributable to Client-controlled or third-party technology.

9. AGREEMENT CONTROLS

9.1 Agreement Controls. The Master Services Agreement, including its payment, confidentiality, intellectual-property, limitation-of-liability, termination, and third-party-provider provisions, applies fully to this Exhibit.

EXHIBIT 2

TRINITY COMPLETE

Fully Managed Information Technology Services

This Exhibit 2 is incorporated into the Master Services Agreement between Trinity Networx, LLC ("Company") and the Client identified in the Agreement. This Exhibit defines the scope, allocation of responsibilities, limitations, and commercial controls applicable to the Trinity Complete Service Plan. Capitalized terms not defined in this Exhibit have the meanings assigned in the Agreement.

1. SERVICE-PLAN PURPOSE

1.1 Fully Managed Service Model. Trinity Complete is a fully managed information technology service plan under which Company serves as Client's primary provider for covered day-to-day information technology support, administration, monitoring, and management.

1.2 Covered Responsibility. Company shall manage covered users, endpoints, network infrastructure, cloud services, and supported technology identified in Company's records, subject to this Exhibit and the Agreement.

1.3 Client Management Contact. Client shall designate an Authorized Contact to approve material changes, purchases, projects, access requests, and other matters requiring Client authorization.

2. INCLUDED END-USER SUPPORT

2.1 Business-Hours Help Desk. Company shall provide reasonable-use remote help desk support to covered users during Normal Business Hours for ordinary incidents and requests involving supported devices, applications, accounts, and services.

2.2 Remote Troubleshooting. Included support may address workstation issues, login problems, printing, approved business applications, Microsoft 365 or Google Workspace, email, network access, and other supported technology.

2.3 Reasonable-Use Limitation. Help desk services described as unlimited remain subject to reasonable and ordinary use and do not include projects, formal training, recurring issues caused by rejected recommendations, unsupported-system remediation, or other excluded work.

2.4 Escalation. Company shall escalate covered incidents through its internal support levels based on severity, complexity, available information, and vendor involvement.

3. INCLUDED MANAGED SERVICES

3.1 Monitoring and Management. Company shall deploy and administer its approved monitoring, management, and inventory tools on supported covered devices.

3.2 Patch Management. Company shall manage generally available operating-system patches and approved third-party application updates when technically and commercially practicable.

3.3 Endpoint Security. Company shall deploy and administer the endpoint security tools identified in Client's Order or applicable service documentation.

3.4 Identity and Access Administration. Company shall provide routine administration of supported user accounts, multifactor authentication, groups, permissions, and access controls within the covered environment.

3.5 Cloud Productivity Administration. Company shall provide routine administration and support for Client's covered Microsoft 365 or Google Workspace environment. Subscription fees and premium licensing are excluded unless expressly stated.

3.6 Network Management. Company shall remotely administer supported covered firewalls, switches, wireless access points, and related network equipment. Manufacturer subscriptions, replacement equipment, cabling, onsite installation, and major reconfiguration are excluded unless expressly included.

3.7 Server Management. Company shall monitor and administer supported servers expressly listed as covered. Server licenses, warranties, cloud consumption, major upgrades, migrations, replacement, and specialized line-of-business support are excluded unless expressly stated.

3.8 Vendor Coordination. Company shall use commercially reasonable efforts to coordinate with approved technology vendors concerning covered incidents. Company is not responsible for a vendor's performance, charges, availability, products, or obligations.

3.9 Documentation and Asset Management. Company shall maintain internal technical documentation and available asset information concerning the covered environment.

4. USER LIFECYCLE SERVICES

4.1 Included Allowance. The Service Plan includes up to two standard user onboardings and two standard user offboardings during each calendar month unless Client's Order states otherwise.

4.2 Standard Onboarding. A standard onboarding generally includes supported account configuration, standard permissions, enrollment of an existing supported device, and installation of approved management and security tools.

4.3 Standard Offboarding. A standard offboarding generally includes disabling supported accounts, revoking access, and completing Company's standard administrative checklist.

4.4 Additional Events. Events exceeding the allowance are billed at $650.00 per additional onboarding and $300.00 per additional offboarding unless the Order states otherwise. Expedited, onsite, equipment, imaging, migration, retrieval, and nonstandard work are separately billable.

5. STRATEGIC AND ADMINISTRATIVE SERVICES

5.1 Technology Reviews. Company shall conduct quarterly business and technology reviews, subject to Client's participation.

5.2 Technology Roadmap. Company shall provide reasonable recommendations concerning lifecycle planning, budgeting, security improvements, and technology priorities.

5.3 Vendor and License Review. Company may assist with covered technology and licensing reviews but does not warrant third-party pricing, terms, or continued availability.

6. CLIENT RESPONSIBILITIES

6.1 Cooperation and Access. Client shall provide timely access, accurate information, appropriate approvals, and reasonable cooperation.

6.2 Authorized Requests. Client shall identify persons authorized to request account changes, access, purchases, projects, and material system modifications.

6.3 Technology Standards. Client shall maintain supported and properly licensed technology and timely implement reasonable security, replacement, and remediation recommendations.

6.4 User Conduct. Client is responsible for user conduct, acceptable-use policies, password practices, data handling, and compliance with Client's legal and contractual duties.

6.5 Change Notification. Client shall notify Company before materially changing personnel, locations, applications, infrastructure, ownership, operations, or regulatory requirements.

7. SERVICES NOT INCLUDED

7.1 Onsite and Premium-Time Work. Onsite, jobsite, travel, after-hours, weekend, and holiday services are excluded unless expressly included and otherwise are separately billable.

7.2 Projects and Major Changes. Projects, migrations, installations, major upgrades, office relocations, construction, low-voltage cabling, and new-location deployments are excluded.

7.3 Products and Third-Party Charges. Hardware, software, cloud consumption, telecommunications, internet, manufacturer support, warranties, and third-party licensing are excluded unless expressly included.

7.4 Business Applications and Databases. Application development, database repair, custom reporting, programming, and specialized vendor support are excluded beyond reasonable vendor coordination and ordinary workstation troubleshooting.

7.5 Backup and Advanced Security. Backup, disaster recovery, 24/7 managed detection and response, SIEM, threat hunting, forensic investigation, and breach response are excluded unless expressly included.

7.6 Compliance and Remediation. Formal compliance, penetration testing, vCISO, written policy development, audit representation, legal advice, preexisting-condition remediation, and technical-debt correction are excluded.

8. SERVICE LIMITATIONS

8.1 Response Versus Resolution. Any stated response target refers to acknowledgment or commencement of triage and is not a guaranteed resolution time.

8.2 Third-Party Dependencies. Company is not responsible for delays, outages, defects, or failures caused by providers, manufacturers, utilities, Client personnel, or other third parties.

8.3 No Guaranteed Outcome. Company does not guarantee uninterrupted operation, elimination of downtime, complete threat prevention, recovery of all data, or compatibility among third-party products.

9. COVERAGE AND ADDITIONAL CHARGES

9.1 Covered Environment. Services apply only to covered users, devices, systems, accounts, and locations recorded by Company and for which applicable fees have been paid.

9.2 Monthly Minimum. Client shall pay the minimum monthly recurring charge stated in the applicable Order regardless of actual usage or user count.

9.3 Out-of-Scope Services. Authorized services outside this Exhibit may be billed at Company's applicable hourly rates or provided under a separate Statement of Work.

EXHIBIT 3

TRINITY COMPLETE SECURE

Fully Managed Information Technology and Advanced Cybersecurity Services

This Exhibit 3 is incorporated into the Master Services Agreement between Trinity Networx, LLC (“Company”) and the Client identified in the Agreement. This Exhibit defines the scope, allocation of responsibilities, limitations, and commercial controls applicable to the Trinity Complete Secure Service Plan. Capitalized terms not defined in this Exhibit have the meanings assigned in the Agreement.

1. SERVICE-PLAN PURPOSE

1.1 Integrated Managed IT and Cybersecurity. Trinity Complete Secure is Company’s comprehensive service plan for Clients requiring fully managed information technology services, enhanced cybersecurity controls, cloud backup, security monitoring, user-security education, and recurring security review.

1.2 Included Managed IT Foundation. This Service Plan includes the fully managed services described in Sections 2 through 6 below and is intended to provide the functional coverage of Trinity Complete together with the enhanced protections stated in this Exhibit.

1.3 Shared Cybersecurity Responsibility. Cybersecurity remains a shared responsibility among Company, Client, Client’s users, and third-party providers. Company’s Services reduce and manage risk but do not eliminate all risk or guarantee that a cybersecurity event will not occur.

2. FULLY MANAGED INFORMATION TECHNOLOGY SERVICES

2.1 Business-Hours Help Desk. Company shall provide reasonable-use remote help desk support to covered users during Normal Business Hours for incidents and requests involving supported technology.

2.2 Monitoring, Management, and Patching. Company shall deploy and administer approved remote monitoring, management, inventory, and patching tools on supported covered devices.

2.3 Cloud Administration. Company shall provide routine administration of Client’s supported Microsoft 365 or Google Workspace environment, including covered account, access, authentication, and configuration functions.

2.4 Network and Server Management. Company shall remotely administer covered and supported servers, firewalls, switches, wireless systems, and related infrastructure identified in Company’s records.

2.5 Vendor Coordination. Company shall use commercially reasonable efforts to coordinate with approved technology vendors concerning covered incidents and services.

2.6 User Lifecycle Services. This Service Plan includes up to two standard onboardings and two standard offboardings per calendar month. Additional standard onboarding is $650.00 per user and additional standard offboarding is $300.00 per user unless the Order states otherwise. Nonstandard work is separately billable.

2.7 Strategic Reviews. Company shall provide quarterly technology and security reviews, subject to Client’s participation.

3. ADVANCED CYBERSECURITY SERVICES

3.1 Managed Endpoint Detection and Response. Company shall deploy and administer its approved endpoint detection and response or managed detection and response platform on supported covered endpoints.

3.2 Security Operations Monitoring. When included in Client’s Order, alerts generated by designated covered security tools may be monitored by Company or an authorized security operations provider. Monitoring applies only to covered data sources and does not constitute review of every event or system.

3.3 Email Security. Company shall administer approved email-security services identified in Client's Order, which may include anti-phishing, malicious-link, attachment, impersonation, and business-email-compromise protections.

3.4 Multifactor Authentication and Conditional Access. Company shall manage supported multifactor-authentication and Conditional Access policies for covered users, subject to licensing, technical compatibility, and approved operational requirements.

3.5 Privileged-Account Review. Company shall periodically review covered administrative and privileged accounts and recommend appropriate changes.

3.6 Dark-Web Credential Monitoring. When included in Client's Order, Company shall monitor designated domains or accounts through its approved credential-monitoring provider. Monitoring does not guarantee discovery of every exposed credential or compromised account.

3.7 Vulnerability Scanning. Company shall perform recurring automated vulnerability scanning of designated covered systems or external assets. Vulnerability scanning is not penetration testing and does not include exploitation, source-code review, physical-security testing, or social engineering.

3.8 Security Awareness Training. Company shall provide covered users access to its approved security-awareness training platform.

3.9 Phishing Simulations. Company shall conduct periodic simulated-phishing exercises using its approved platform. Client shall cooperate with enrollment, communications, and corrective training.

3.10 Security Reporting. Company shall provide periodic reporting concerning covered security tools, identified risks, training participation, and recommended corrective actions.

4. BACKUP AND BUSINESS CONTINUITY SERVICES

4.1 Cloud-Productivity Backup. When included in Client's Order, Company shall administer backup services for designated Microsoft 365 or Google Workspace data. Protected workloads, retention, capacity, and restoration capabilities are limited to the selected platform and licensing.

4.2 Endpoint Backup. When expressly included, Company shall administer endpoint backup for designated devices, subject to the storage allowance, retention period, file-type limitations, and requirements stated in Client's Order.

4.3 Restoration Assistance. Company shall provide reasonable assistance with standard restoration requests involving covered backup data. Large-scale, emergency, forensic, or disaster-recovery restorations may be separately billed.

4.4 Restoration Testing. Company shall periodically test restoration of selected covered backup data under Company's procedures. Representative testing does not verify every file, account, system, or recovery scenario.

4.5 Client Verification. Client remains responsible for identifying the data and systems requiring protection and informing Company of legal, contractual, retention, recovery-time, or recovery-point requirements.

5. SECURITY PLANNING AND RISK MANAGEMENT

5.1 Annual Cybersecurity Assessment. Company shall conduct an annual assessment of the covered environment using Company's standard assessment methodology.

5.2 Incident-Response Planning. Company shall provide standard incident-response planning guidance and facilitate one annual tabletop exercise when included in Client's Order.

5.3 Cyber-Insurance Assistance. Company may assist Client in gathering information concerning covered systems and controls. Company is not Client's broker, attorney, auditor, or guarantor and does not warrant insurance eligibility, coverage, or application sufficiency.

5.4 Remediation Recommendations. Company may identify and recommend security improvements. Unless expressly included, implementation, hardware, licensing, projects, and remediation are separately chargeable.

6. CLIENT SECURITY RESPONSIBILITIES

6.1 Compliance With Security Controls. Client shall implement and enforce reasonable security recommendations, including multifactor authentication, supported software, secure access, timely account termination, training, and replacement of obsolete technology.

6.2 Incident Notification. Client shall immediately notify Company of suspected unauthorized access, phishing, fraud, data loss, malware, stolen equipment, credential compromise, or other suspected security incidents.

6.3 Transaction Verification. Client shall independently verify payment instructions, banking changes, wire requests, payroll changes, and other sensitive transactions through an approved out-of-band procedure.

6.4 User Participation. Client shall require covered users to complete assigned training and follow Client's security, acceptable-use, data-handling, and access-control policies.

6.5 Regulatory Requirements. Client shall identify all laws, regulations, customer requirements, contractual security obligations, retention duties, and industry standards applicable to Client.

7. SERVICES NOT INCLUDED

7.1 Onsite, After-Hours, and Projects. Onsite work, jobsite visits, travel, after-hours end-user support, projects, migrations, installations, relocations, new-location deployments, structured cabling, and major upgrades are excluded unless expressly included.

7.2 Products and Third-Party Charges. Hardware, software, cloud consumption, telecommunications, internet, warranties, manufacturer support, and third-party licensing not expressly identified as included are excluded.

7.3 Advanced Testing and Investigation. Formal penetration testing, red-team exercises, source-code review, physical-security testing, digital forensics, legal investigation, e-discovery, breach counsel, regulatory notification, ransom negotiation, and law-enforcement liaison are excluded.

7.4 Compliance and vCISO Services. CMMC, NIST, HIPAA, PCI, or other certification; formal attestations; compliance audits; vCISO services; written policy development; and audit representation are excluded unless separately authorized.

7.5 Preexisting Conditions and Specialized Applications. Remediation of preexisting vulnerabilities, technical debt, compromised accounts, data corruption, and specialized construction-management, accounting, database, estimating, or other line-of-business application work are excluded beyond reasonable vendor coordination and ordinary troubleshooting.

8. CYBERSECURITY LIMITATIONS

8.1 No Absolute Security. No cybersecurity program, monitoring service, backup platform, access control, or protective technology can prevent or detect every threat, intrusion, error, fraud, vulnerability, or loss.

8.2 Covered Systems Only. Cybersecurity services apply only to covered users, accounts, devices, systems, domains, and data sources properly licensed, configured, and enrolled in Company's approved tools.

8.3 Third-Party Platforms. Company is not responsible for defects, outages, breaches, data loss, service changes, or failures originating in third-party products or services outside Company's reasonable control.

8.4 Client Decisions. Company is not responsible for losses arising from Client's rejection, delay, modification, disabling, or circumvention of a recommended security control.

8.5 Services Are Not Insurance. The Services are not insurance and do not transfer to Company the business, financial, legal, or regulatory consequences of a cybersecurity event.

9. COVERAGE AND ADDITIONAL CHARGES

9.1 Covered Environment. Services apply only to covered users, devices, systems, accounts, domains, data sources, and locations recorded by Company and for which applicable fees have been paid.

9.2 Monthly Minimum. Client shall pay the minimum monthly recurring charge stated in the applicable Order regardless of actual usage or user count.

9.3 Additional Security and Compliance Services. Advanced SIEM, extended log retention, managed threat hunting, vCISO, formal compliance, penetration testing, digital forensics, incident response, and other specialized services require a separate Statement of Work.

9.4 Out-of-Scope Services. Authorized services outside this Exhibit may be billed at Company's applicable hourly rates or provided under a separate Statement of Work.